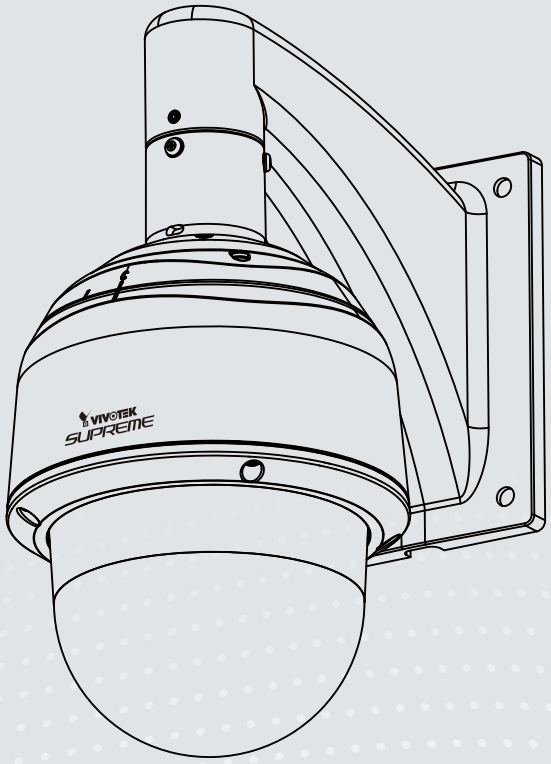
SD8333-E/M Speed Dome Network Camera

User's Manual

720P • 30x Zoom • NEMA 4x • IP67 •
Extreme Weatherproof



Rev. 1.1

SUPREME

Table of Contents

Overview *4*

Revision History 4
Read Before Use 5
Package Contents 5
Symbols and Statements in this Document 5
Physical Description *6*

Installation - for the Configuration w/ Extended Cables *9*

Hardware Installation *9*

Network Deployment 14
Software Installation 17
Ready to Use 18

Accessing the Network Camera *19*

Using Web Browsers 19
Using RTSP Players 21
Using 3GPP-compatible Mobile Devices 22
Using VIVOTEK Recording Software 23

Main Page *24*

Client Settings *30*

Configuration *35*

System > General settings 36
System > Homepage layout 37
System > Logs 40
System > Parameters 41
System > Maintenance 42
Media > Image 46
Media > Video 56
Media > Audio 59
Network > General settings 60
Network > Streaming protocols 68
Network > DDNS 72
Network > SNMP (Simple Network Management Protocol) 77
Security > User Account 78
Security > HTTPS (Hypertext Transfer Protocol over SSL) 79
Security > Access List 86
PTZ > PTZ settings 91
Event > Event settings 96
Applications > Motion detection 111
Applications > DI and DO 114
Applications > Audio detection 115
Applications > VADP (VIVOTEK Application Development Platform) 117

Recording > Recording settings 119
Local storage > SD card management 124
Local storage > Content management 125
Appendix 127
URL Commands for the Network Camera 127
Technical Specifications 222
Technology License Notice 223
Electromagnetic Compatibility (EMC) 224

Overview

VIVOTEK SD8333-E is part of the SUPREME series product line offering 720p HD resolution with superb image quality. Adopting a 30x optical zoom lens, the SD8333-E is able to capture details at top-notch quality. The IP67- and NEMA 4X-rated housing protects the camera body against rain, dust and corrosion within a wide temperature range between -40°C to 55°C. This feature ensures operation under extreme weather conditions and hazardous environments. It is especially suitable for monitoring wide open indoor/outdoor spaces such as airports, highways and parking lots where high-level reliability and precision are always required.

The SD8333-E supports high-performance H.264/MPEG-4/MJPEG compression technology and offers extra smooth video quality with resolution up to 60 fps @ 720p. Boasting WDR Pro technology, the SD8333-E can also cope with challenging lighting conditions and generate image quality close to the capabilities of the human eye. With a sophisticated pan/tilt mechanism, the camera provides fast, precise movement with continuous 360-degree pan and 220-degree tilt. Users can also easily control the lens position via a mouse or a joystick to track the object of interest and set up to 256 preset positions. With the built-in auto tracking feature, the SD8333-E provides instantaneous reaction to suspicious moving objects in wide area locations before operators are aware of activity.

Revision History

- Rev. 1.0: Initial release
- Rev. 1.1: Updated technical specifications and DI/DO pin definitions.

IMPORTANT:

1. The camera can be driven by an Ethernet connection to a PoE Plus switch (30W output). You can connect both the PoE Plus and the 24V power for fail-safe redundancy.
2. If the installation requires heating in the winter (<-5ºC), you require approximately 60 Watts of power to drive the embedded heater. You can connect either or both of the 24V power lines or a High Power PoE power injector (separately purchased).

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/ surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

Package Contents

- SD8333-E/ -M (-M specifies the camera that comes with an electronic dehumidifier unit)
- Wall Mount Bracket / Screws
- Waterproof Connectors / Terminal Blocks / Ethernet Cable / Ground Wire
- Screws / Alignment Sticker / T25 Stardriver / Seal Ring / Desiccant Bags
- Quick Installation Guide
- Software CD / Warranty Card
- PC/ABS /Smoked Dome Cover / IO Combo Cable (may come with one 1m combo cable or Separately Purchased)

Symbols and Statements in this Document

INFORMATION: provides important messages or advices that might help prevent inconvenient or problem situations.

NOTE: Notices provide guidance or advices that are related to the functional integrity of the machine.

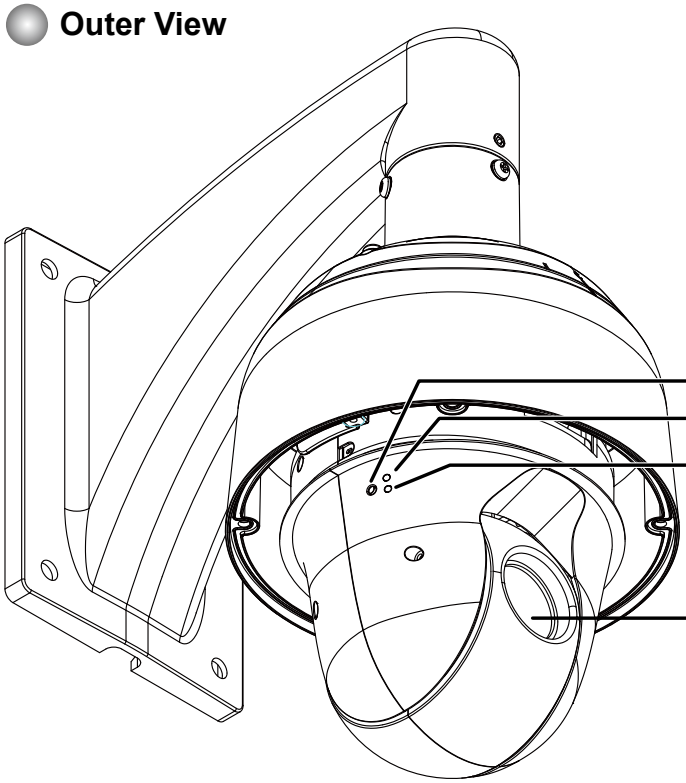
Tips: Tips are useful information that helps enhance or facilitae an installation, function, or process.

WARNING: or IMPORTANT:: These statements indicate situations that can be dangerous or hazardous to the machine or you.

Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

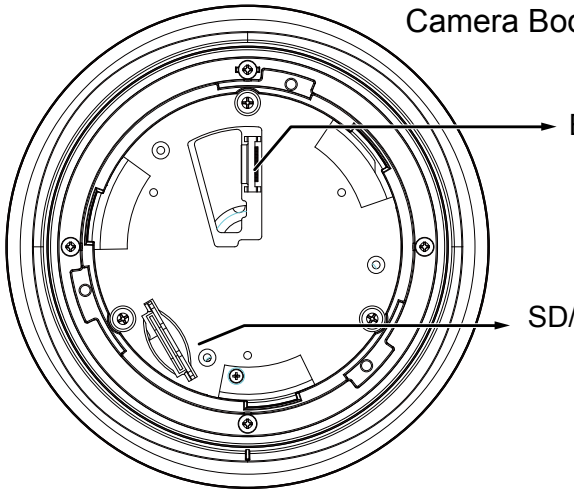
Physical Description

Outer View

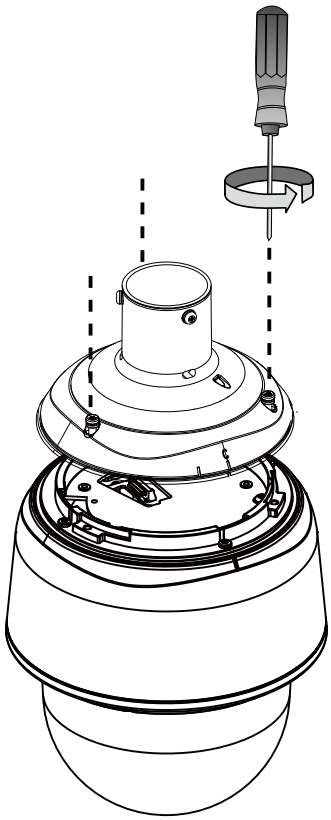


This drawing shows a camera with its dome cover removed.

Inner View



The card slot is accessed by removing the top section using the T25 stardriver.



Status LED

Item	LED status	Description
1	Steady red	Power on and system booting
	Red LED OFF	Power off
2	Steady red & Green blinking every 1 sec.	Network normal (heartbeat)
	Steady red & Green LED OFF	Network failed
3	Red blinking every 0.15 sec. & Green blinking every 1 sec.	Upgrading firmware
4	Red blinking every 0.15 sec. & Green blinking every 0.15 sec.	Restoring default

Hardware Reset

The reset button is used to reset the system or to restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

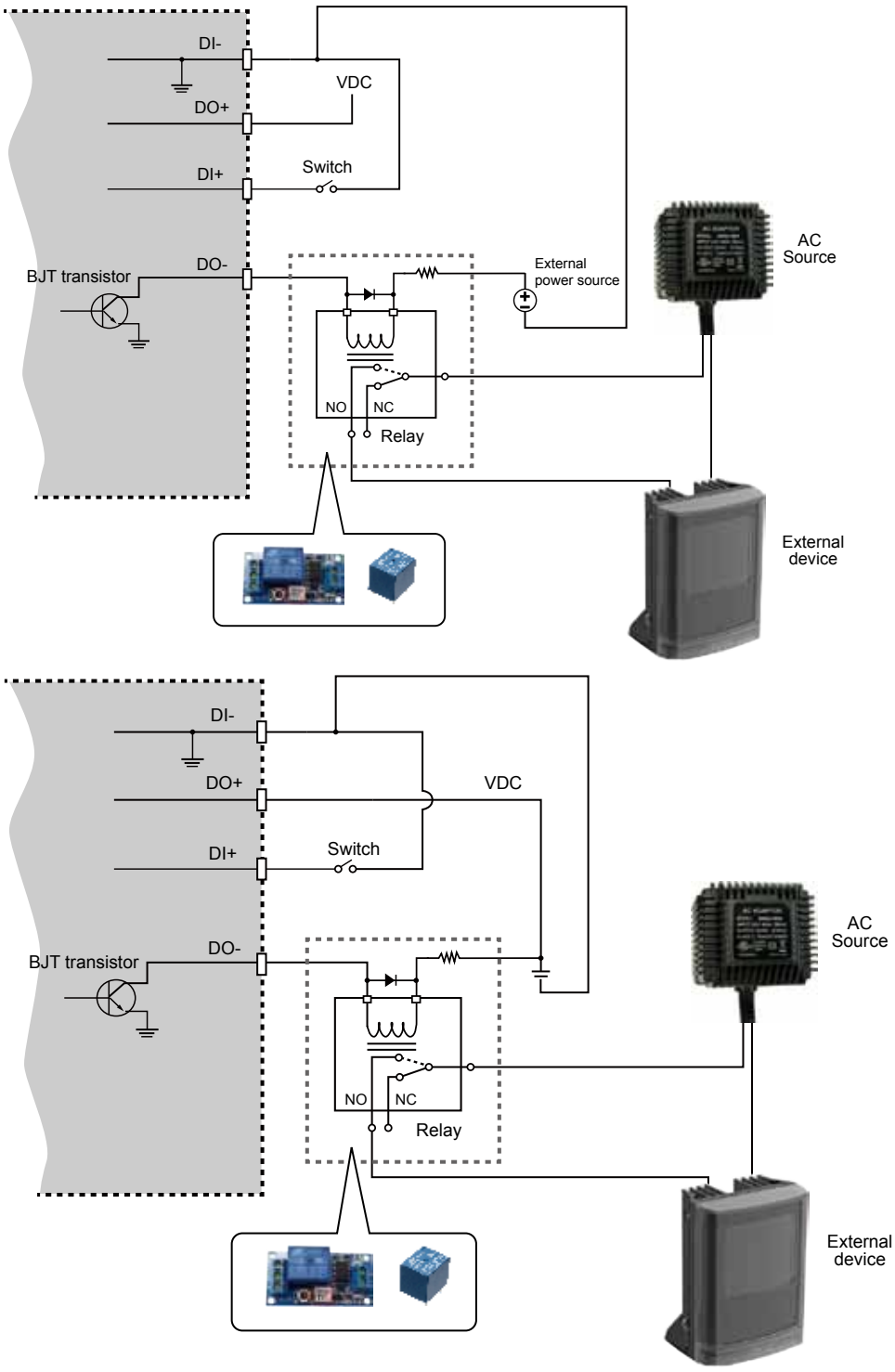
Reset: Press and release the reset button with a paper clip or thin object. Wait for the Network Camera to reboot.

Restore: Press and hold the reset button for at least ten seconds to restore system defaults. Note that all settings will be restored to factory defaults.

SD/SDHC/SDXC Card Capacity

This network camera is compliant with **SD/SDHC/SDXC 32GB, 64GB,** and other preceding standard SD cards.

DI/DO Diagram



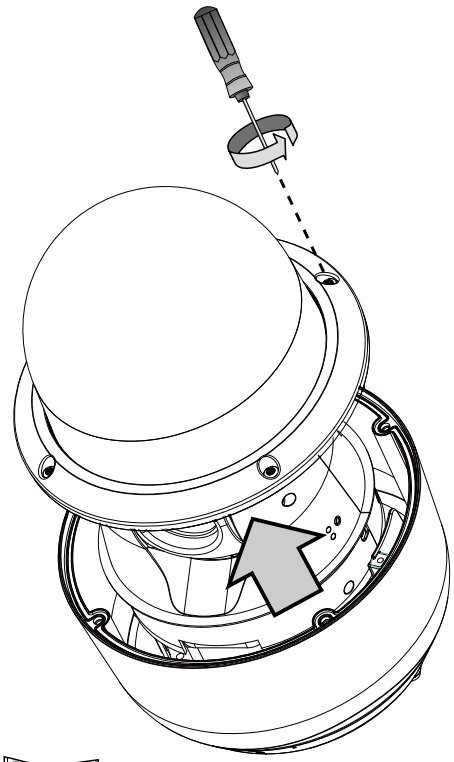
1. The DO+ pin provides 12V output voltage, and the max. load is 50mA.
2. The max. voltage for DO- pins is 80VDC (External power).
   In order to control AC devices, the above diagram can be taken in consideration. The diagram uses a relay to control the ON/OFF condition of the AC device.
3. An external relay can be triggered by using DO+ or by an external power source, depending on the type of relay you use.
4. In case of using an individual relay (instead of using a relay module), for protection against voltage or current spikes, a transient voltage suppression diode must be connected in parallel with the inductive load.

Installation - for the Configuration w/ Extended Cables

Hardware Installation

IMPORTANT:

If your camera comes without the dehumidifier, you should examine whether the color of the silica gel inside the chassis has turned dark. If so, you should replace the desiccant bag.

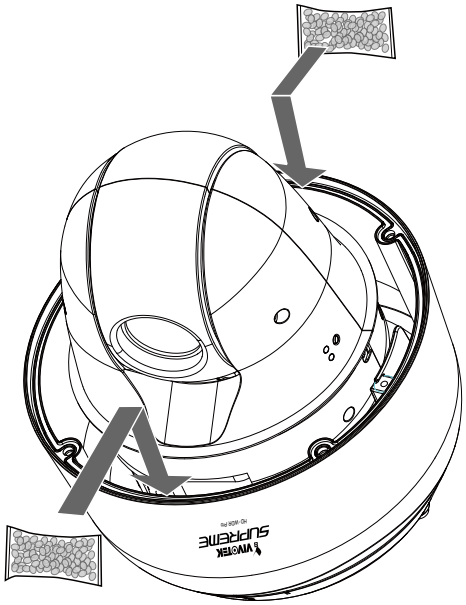


To replace the desiccant bags:

1. Remove the dome cover by loosening 4 T25 anti-tamper screws.
2. Replace the desiccant bags by attaching them firmly to the inside of the chassis.
3. Re-install the dome cover.

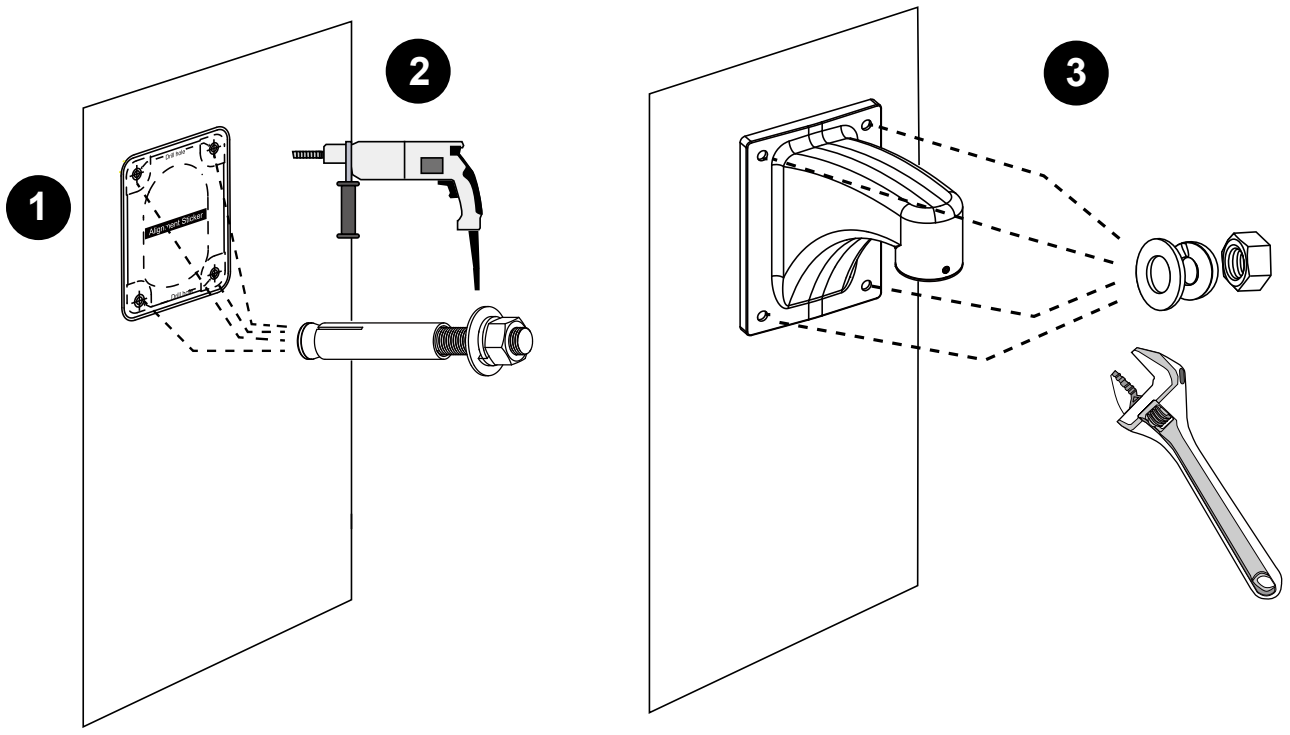
Also note the following:

1. Do not install the camera in a raining day.
2. It takes approximately 2 days to suppress the moisture level to 30% or lower, either using the desiccant bags or the dehumidifier.
3. Condensation may still be observed from on the dome cover within 30 minutes.



Install the Wall-mount Bracket

1. The camera weighs 3.66 kgs. Select a rigid mounting location to prevent vibration to the camera. Attach the alignment sticker to the wall.
2. Drill 4 pilot holes (10mm in diameter and 4cm deep) into the wall, and then hammer in the threaded anchors. Note that you should hammer the anchors with hex nuts on them so that the threaded poles will not be deformed! If preferred, drill another hole for routing cables.
3. Secure the wall mount bracket to wall using 4 sets of captive washers and nuts.

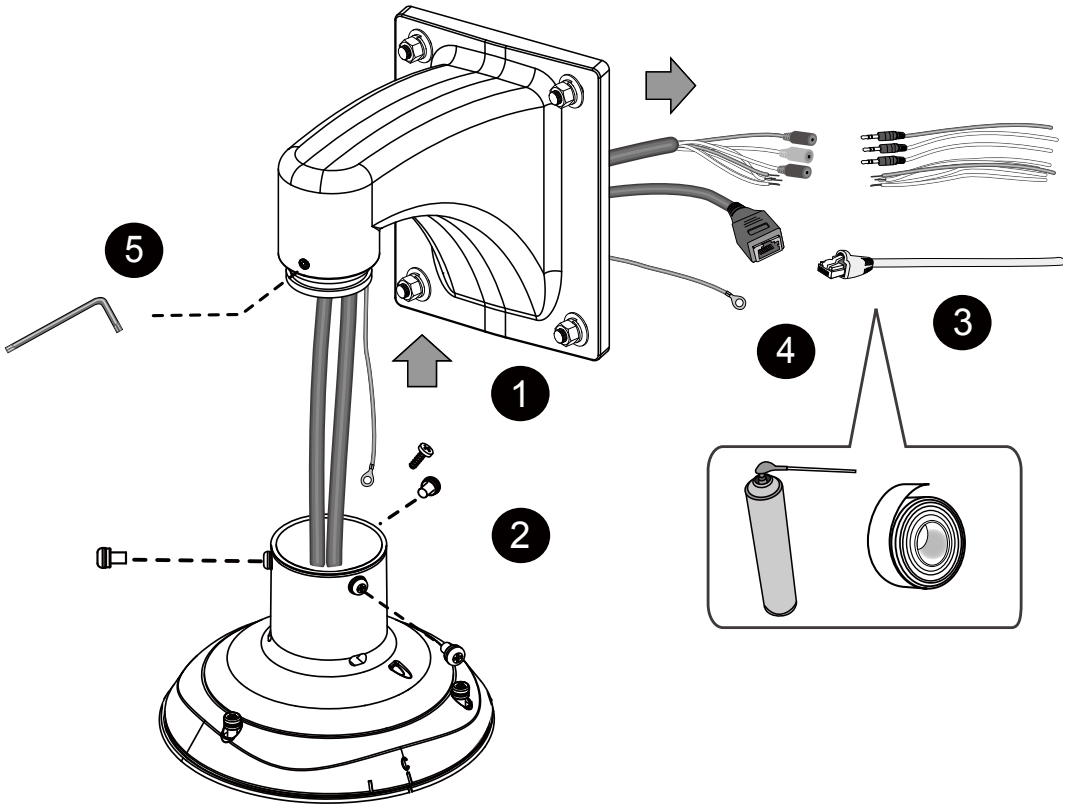


NOTE:

1. IO wires are user-supplied.
2. Avoid touching the circuit boards to prevent damage by electro static discharge.
3. Use CAT5e, CAT6 cables only.

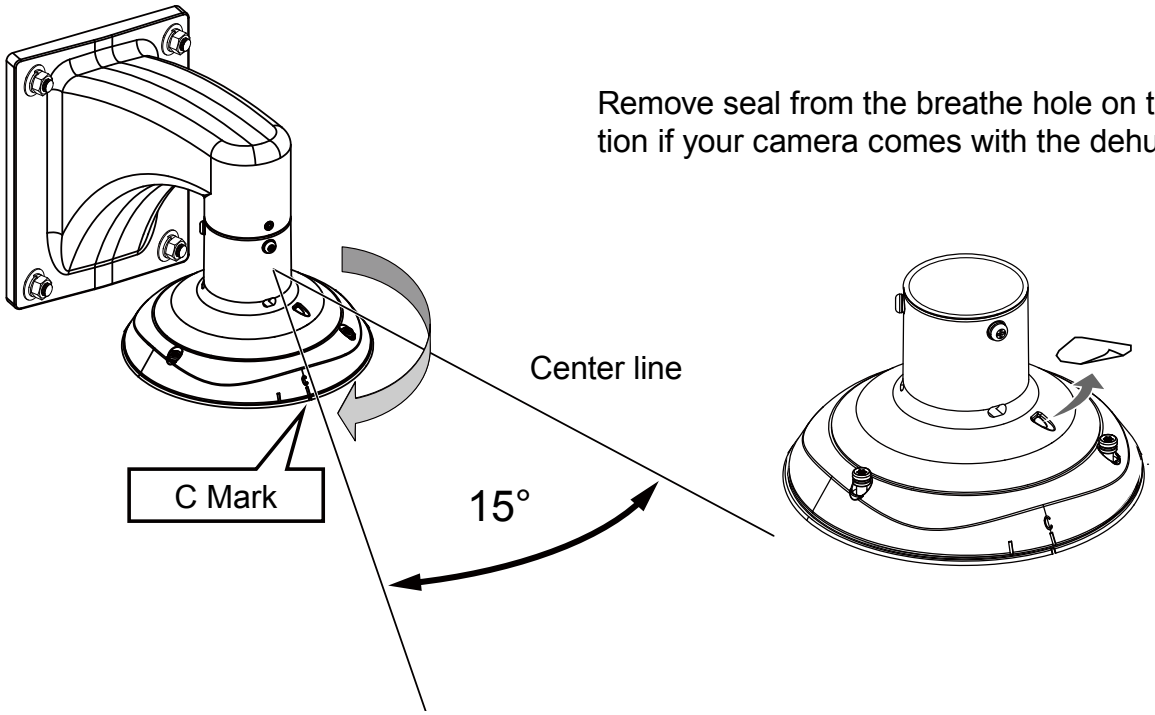
Cabling Connections & Attach the Top Section

1. Hold your top section with one hand and pass all cables through the wallmount bracket.



2. Secure the top section to the wall mount bracket.

Note that you should turn and orient the top section so that the C mark is facing a direction 15 degrees off the center line.

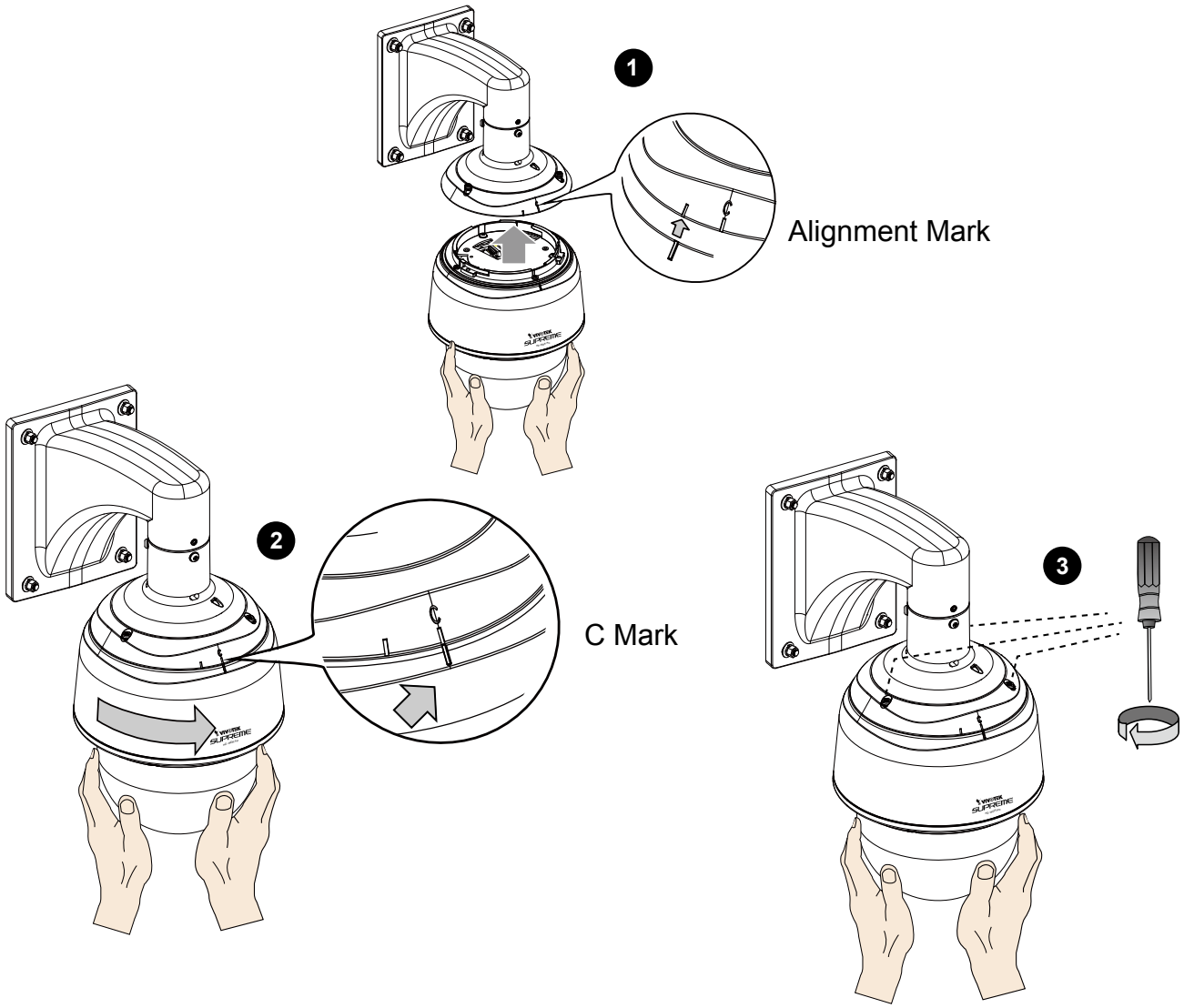


Remove seal from the breathe hole on the top section if your camera comes with the dehumidifier.

3. Connect cables and use sealants and putties to make sure cable joints and the cabling hole are waterproof.
4. Secure the included ground wire to the dome cap, pass it through the mount bracket, and connect the other end to a grounded conduit later.
5. Use the included hex wrench to secure the top section.

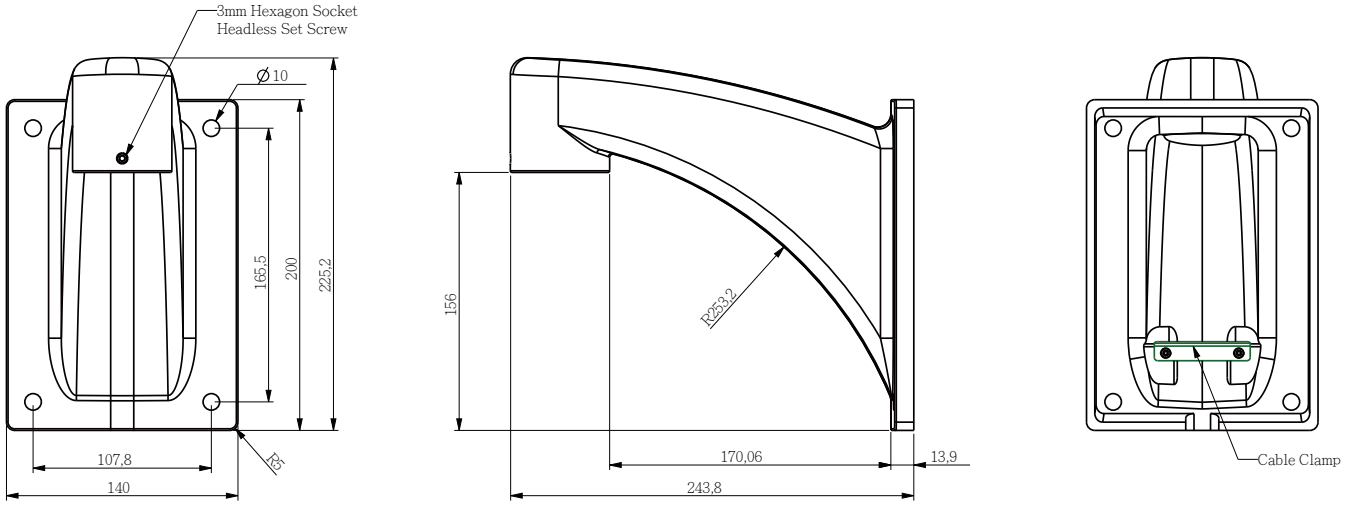
Mounting the Camera

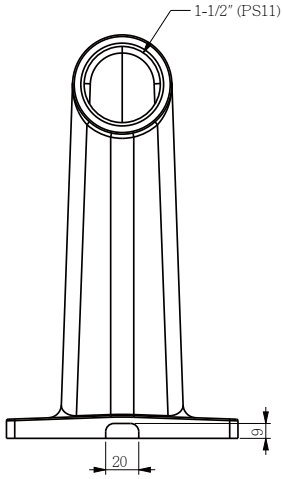
1. Align the camera body with the top section. Align the alignment mark on the camera with that on the interface section. Push the camera up to match the top section.
2. Rotate the camera clockwise until its alignment mark is aligned with the "C" mark.
3. Use the included T25 stardriver to tighten the 3 anti-tamper screws from the top. Make sure all parts have been securely tightened.



Mechanical Dimensions

Shown below are the dimensions of the wall mount bracket and its mounting holes:





You can find the installation instructions on VIVOTEK's website for other options such as parapet mount: http://www.vivotek.com/web/product/accessories.aspx

NOTE:

Before mounting the camera, install an SD card if you prefer recording to local storage.

Network Deployment

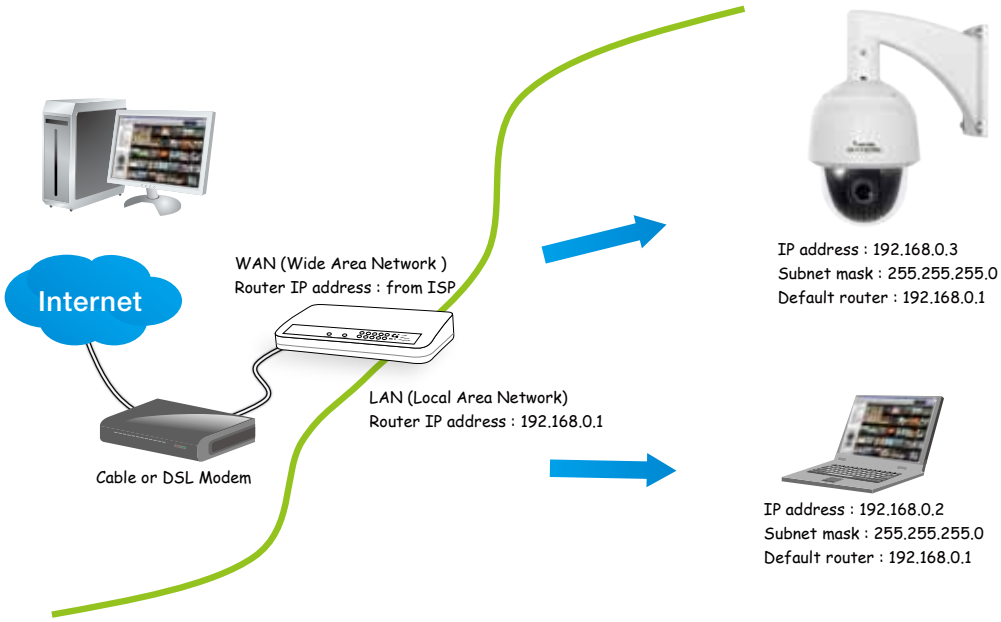
Setting up the Network Camera over the Internet

There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 17 for details.


Internet
WAN (Wide Area Network)
Router IP address : from ISP
LAN (Local Area Network)
Router IP address : 192.168.0.1
Cable or DSL Modem
IP address : 192.168.0.3
Subnet mask : 255.255.255.0
Default router : 192.168.0.1
IP address : 192.168.0.2
Subnet mask : 255.255.255.0
Default router : 192.168.0.1

2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

   - Secondary HTTP port: 8080
   - RTSP port: 554
   - RTP port for audio: 5558
   - RTCP port for audio: 5559
   - RTP port for video: 5556
   - RTCP port for video: 5557

If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the

Internet. Please refer to Network Type on page 60 for details.

For example, your router and IP settings may look like this:

Device	IP Address: internal port	IP Address: External Port (Mapped port on the router)
Public IP of router	122.146.57.120	
LAN IP of router	192.168.2.1	
Camera 1	192.168.2.10:80	122.146.57.120:8000
Camera 2	192.168.2.11:80	122.146.57.120:8001
...	...	...

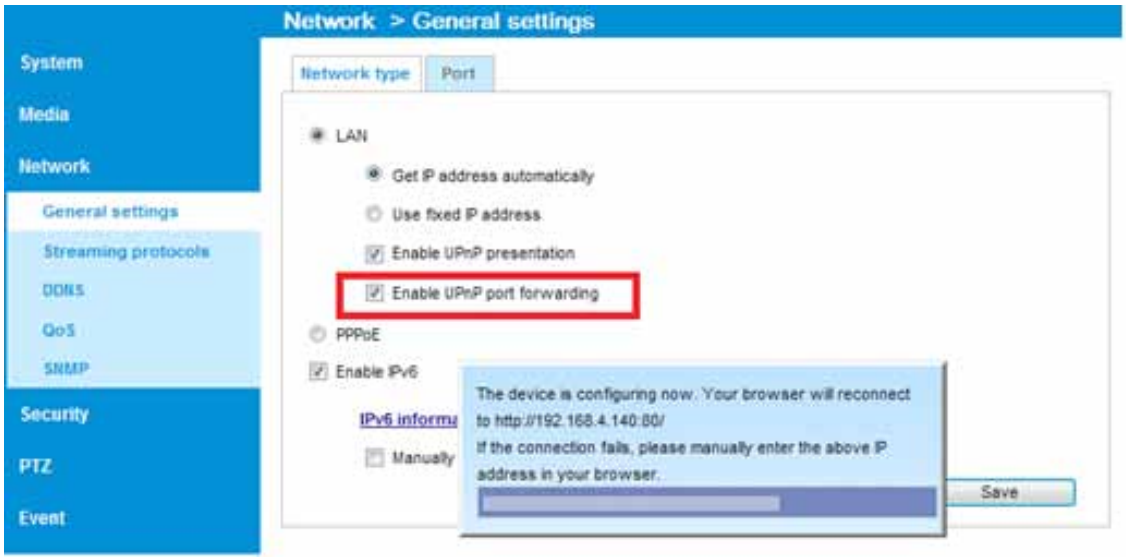
Configure the router, virtual server or firewall, so that the router can forward any data coming into a preconfigured port number to a network camera on the private network, and allow data from the camera to be transmitted to the outside of the network over the same path.

From	Forward to
122.146.57.120:8000	192.168.2.10:80
122.146.57.120:8001	192.168.2.11:80
...	...

When properly configured, you can access a camera behind the router using the HTTP request as follows: http://122.146.57.120:8000

If you change the port numbers on the Network configuration page, please open the ports accordingly on your router. For example, you can open a management session with your router to configure access through the router to the camera within your local network. Please consult your network administrator for router configuration if you have troubles with the configuration.

For more information with network configuration options (such as that of streaming ports), please refer to Configuration > Network Settings. VIVOTEK also provides the automatic port forwarding feature as an NAT traversal function with the precondition that your router must support the UPnP port forwarding feature.



Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN on page 60 for details.

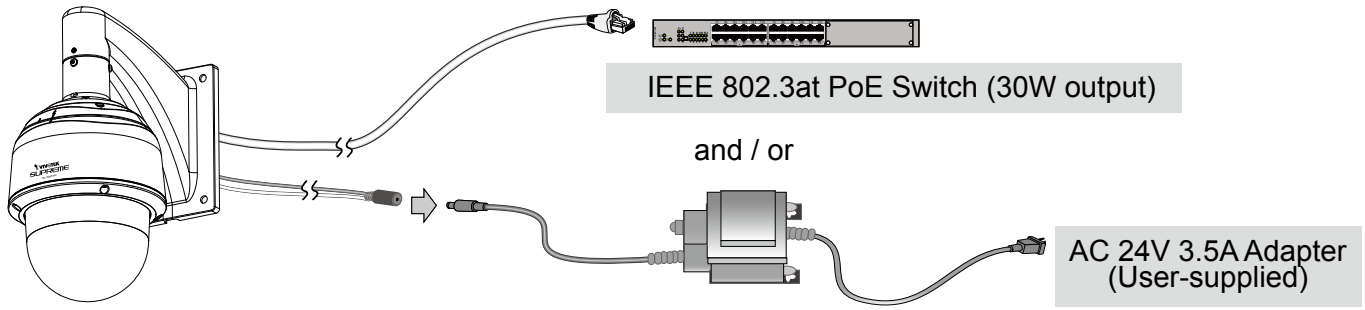
Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 61 for details.

General Connection

1. Connect the Network Camera's Ethernet cable (CAT5e) to a PoE Plus switch. A 30W PoE output port alone can not drive the onboard heater, and hence if using the PoE switch alone, the application does not apply in low-temperature condition. 30W PoE plus can only drive the camera when it is working at a temperature higher than -5ºC.
2. Connect the power wires to an AC 24V power adaptor (user-supplied). The AC 24V adapter can drive the camera and the onboard heater.

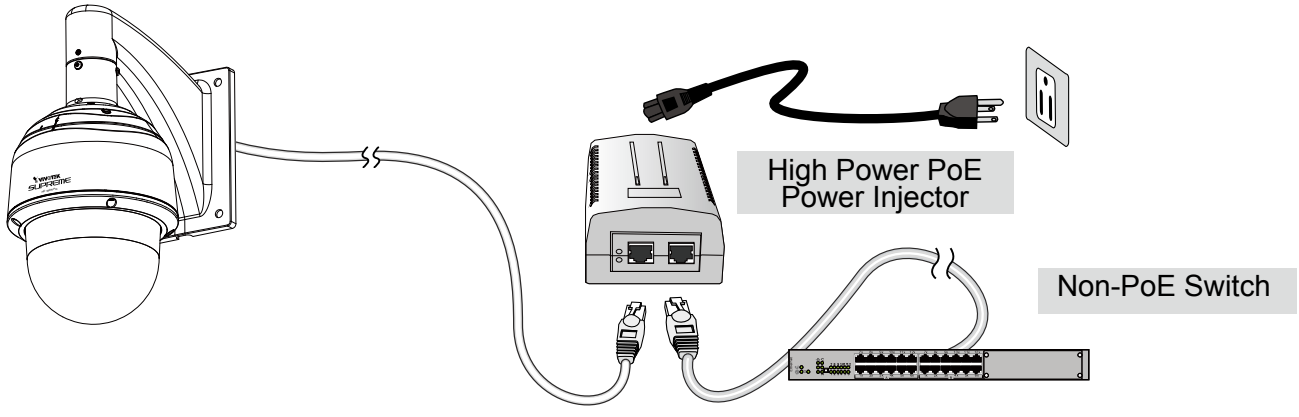
You can connect both power sources for redundancy in power supply.



Power over Ethernet (High Power PoE)

When using a non-PoE switch

Use a High Power PoE power injector (separately purchased) capable of 60W output to connect between the Network Camera and a non-PoE switch. Sufficient power is required for low temperature conditions when the onboard heater is activated.



Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

1. Install IW2 under the Software Utility directory from the software CD. Double click the IW2 shortcut on your desktop to launch the program.

2. The program will conduct an analysis of your network environment. After your network environment is analyzed, please click **Next** to continue the program.

3. The program will search for all VIVOTEK network devices on the same LAN.

4. After a brief search, the main installer window will prompt. Double-click on the MAC and model name which matches the product label on your device to connect to the Network Camera via a web browser.

Device Selection
Installation Wizard 2
Smart Setup
Refresh Devices
MAC
IP Address
Model
00-02-D1-73-02-02
192.168.5.151
SD8333E
0002D1730202
Please check the MAC and model name in the product label of your device first. Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list.
If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.
You can find the product label in the rear/bottom part of your device.

Ready to Use

1. A browser session with the Network Camera should prompt as shown below.
2. You should be able to see live video from your camera. You may also install the 32-channel recording software from the software CD in a deployment consisting of multiple cameras. For its installation details, please refer to its related documents.

⚠ IMPORTANT:

- *Currently the Network Camera utilizes a **32-bit ActiveX plugin**. You **CAN NOT** open a management/view session with the camera using a 64-bit IE browser.*
- *If you encounter this problem, try execute the Iexplore.exe program from C:\Windows\SysWOW64. A 32-bit version of IE browser will be installed.*
- *On Windows 7, the 32-bit explorer browser can be accessed from here: C:\Program Files (x86)\Internet Explorer\iexplore.exe*
- *If you experience compatibility issues between the plug-in control, you may try to uninstall the Camera Stream Controller located in: C:/Program Files (x86)/Camera Stream Controller.*

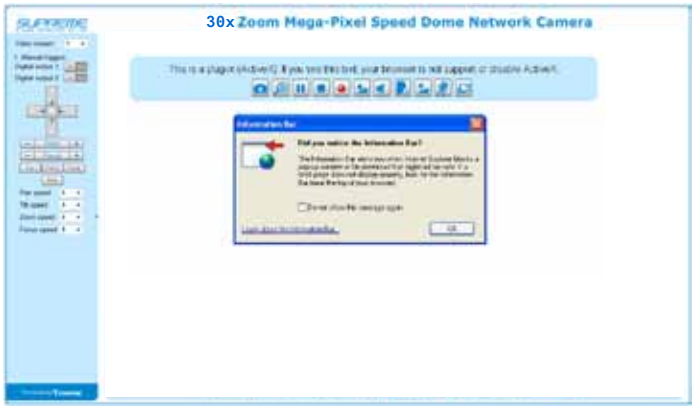
Accessing the Network Camera

This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access to the Network Cameras on the LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:

1. Launch your web browser (e.g., Microsoft® Internet Explorer or Mozilla Firefox).
2. Enter the IP address of the Network Camera in the address field. (A temporary IP will be generated for the camera. Find it in your Network Neighborhood). Press **Enter**.
3. Live video will display in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.



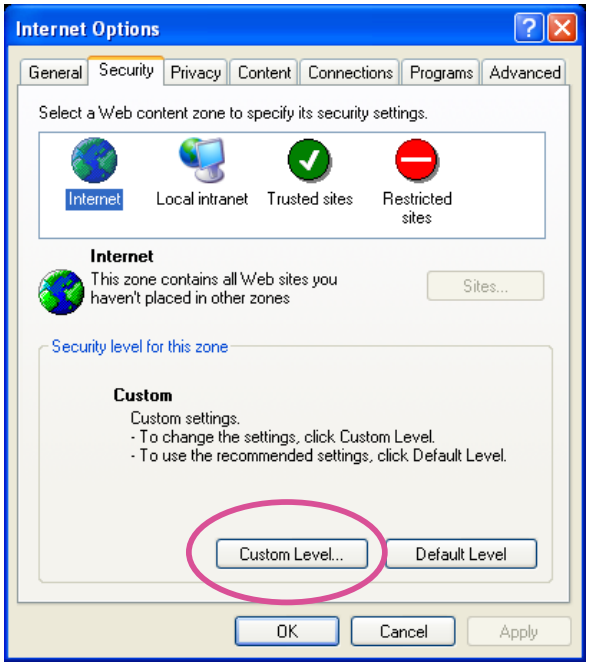
NOTE:

*For Mozilla **Firefox** or **Netscape** users, your browser will use **Quick Time** to stream live video. If you do not have Quick Time on your computer, please download Quick Time from Apple Inc's website, and then launch your web browser.*

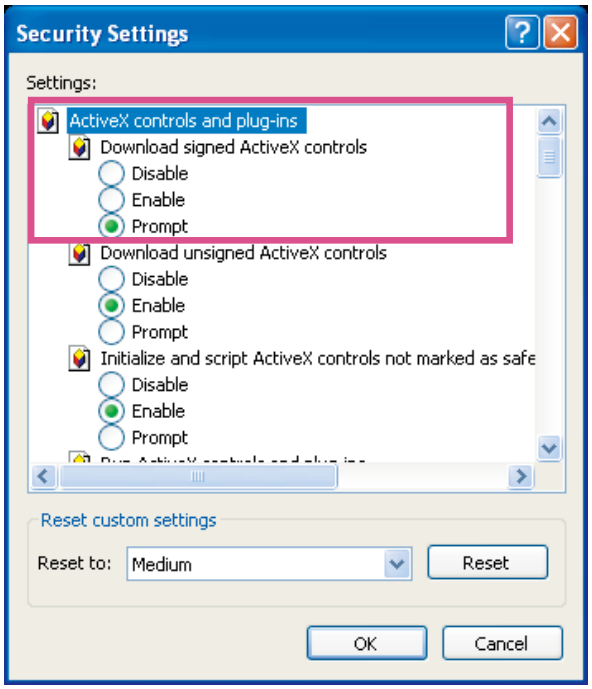
► *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 78.

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



*2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.*



3. Refresh your web browser, then install the ActiveX® control. Follow the instructions to complete installation.

Using RTSP Players

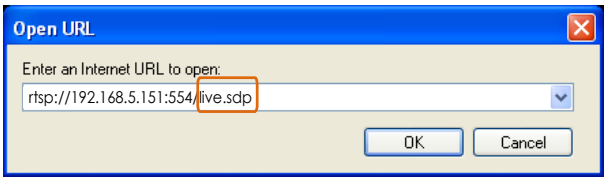
To view the H.264/MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

VLC Media Player

1. Launch the RTSP player.
2. Choose File > Open URL. An URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 69.
For example:



4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 69 for details.

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 14.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 69.

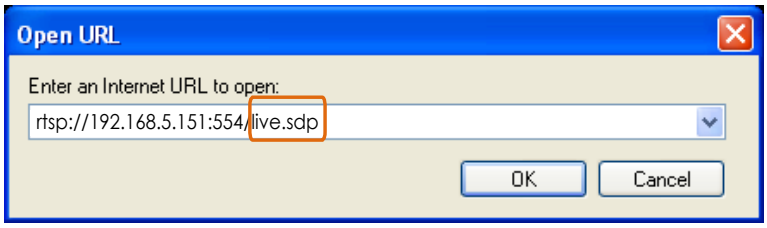
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Stream settings on page 57.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 69.

4. Launch the player on the 3GPP-compatible mobile devices (ex. Real Player).

5. Type the following URL commands into the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>.
   For example:



Using VIVOTEK Recording Software

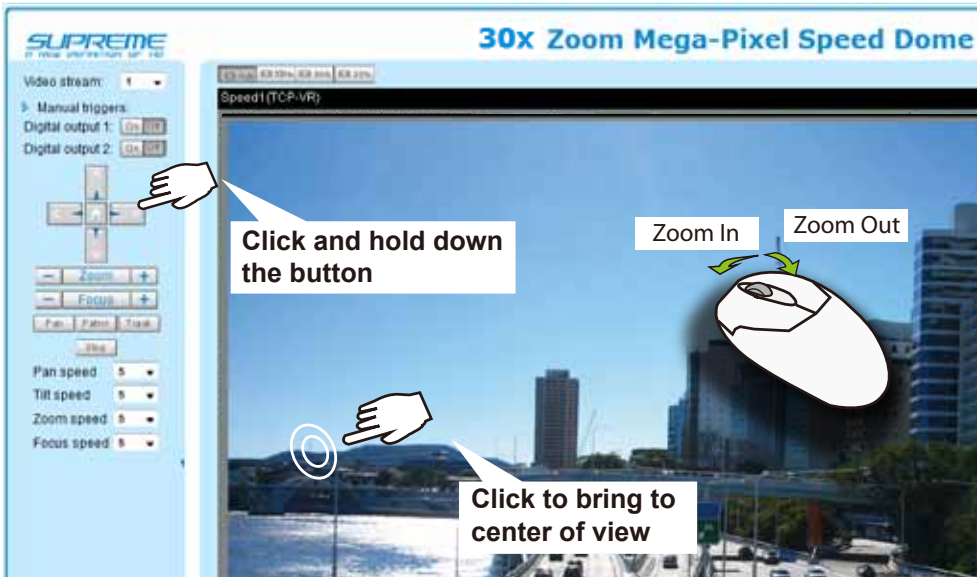
The product software CD also contains recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it from http://www.vivotek.com.

Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, and Live Video Window.

Mouse and Screen Control

In addition to the use of a joystick, mouse control is also supported by the web session. You can click on any spot on the screen to move camera's field of view to that direction. To pan 360 degrees, you can click and hold down the left mouse button when clicking a PTZ button. The same applies to arrow keys, Zoom, and Focus buttons on the PTZ panel.



Note that if your screen control malfunctions, it is possible that the CPU of your current view station can not cope with the HD video feeds or that an incompatibility issue occurred with the ActiveX control plug-ins.

VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 36.

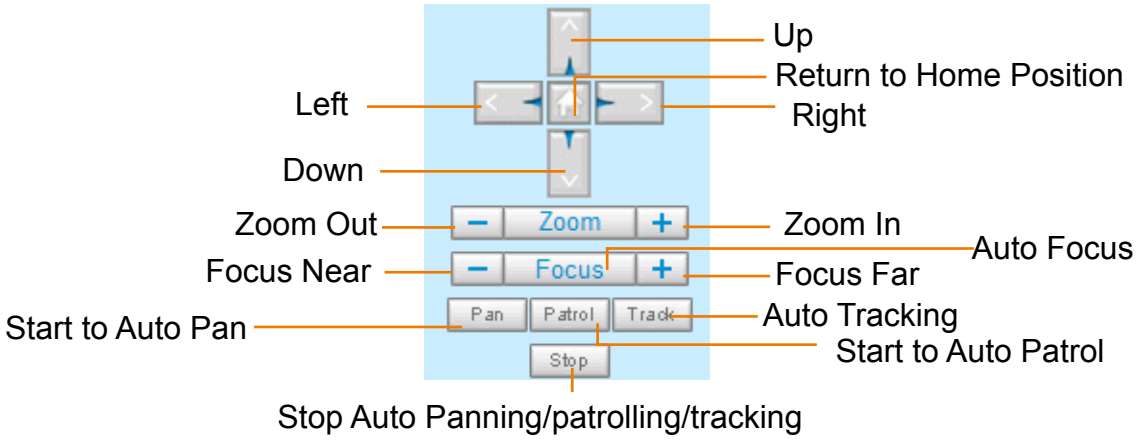
Camera Control Area

Video Stream: This Network Camera supports multiple streams (stream 1 ~ 4) simultaneously. You can select either one for live viewing. For more information about multiple streams, please refer to page 56 for detailed information.

Manual triggers: Manual triggers can be turned on/off by users from the main page. The manual triggers can be associated with the Event settings, and, as the result, can be used to perform recording actions, sending notifications, and so on. See Event settings on page 96.

Digital Output: Click to turn the digital output device on or off.

PTZ Control Panel:



Pan: Click this button to start the auto pan (360° continuous rotation).

Stop: Click this button to stop the Auto Pan, Auto Patrol, and Auto Tracking functions.

Patrol: Once the Administrator has determined the list of preset positions (including the zoom-in action on a particular position), click this button to command the camera to patrol among those positions on the Patrol List. The Network Camera will patrol continuously. For more information, please refer to PTZ control on page 91.

Track: Allows the camera to move along following the moving objects in the current field of view. If you observe an object of your interest, click this button to track the object. Note that this function does not apply in an extremely crowded area, such as a market or sidewalk full of pedestrian activities. Constant shift of tracked objects will decrease the usability of this feature.

Once started, you can use the Stop button to stop the current action. A click on the screen can also stop the tracking action.

Another key concept is that the camera only detect movements within the current field of view.

Please refer to **PTZ** > **Auto tracking** on page 94 and further for tracking configuration details.

Pan /Tilt /Zoom /Focus speed: Adjust the speed of Pan/ Tilt/ Zoom/ Focus:

Pan speed	Tilt speed	Zoom speed	Focus speed	
-5	-5	-5	-5	Slower
-4	-4	-4	-4	
-3	-3	-3	-3	
-2	-2	-2	-2	
-1	-1	-1	-1	
0	0	0	0	
1	1	1	1	
2	2	2	2	
3	3	3	3	Faster
4	4	4	4	
5	5	5	5	

Note that mouse screen control is also supported. You can refer to page 91 for related information.

Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 30.

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 35.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文. You can also change a language on the Configuration page; please refer to page 35.

Hide Button

You can click the hide button to hide the control panel or display the control panel.

Resize Buttons

:
Click the Auto button, the video cell will resize automatically to fit the monitor.
Click 100% is to display the original homepage size.
Click 50% is to resize the homepage to 50% of its original size.
Click 25% is to resize the homepage to 25% of its original size.

Go to

If you have preset PTZ positions, these positions will be available in the Go to menu. Please refer to page 91 for more information.

Live Video Window

■ The following window is displayed when the video mode is set to H.264 / MPEG-4:

Video Title: The video title can be configured. For more information, please refer to Video settings on page 46.

H.264 / MPEG-4 Protocol and Media Options: The transmission protocol and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 30.

Time: Display the current time. For further configuration, please refer to Media > Image > General settings on page 46.

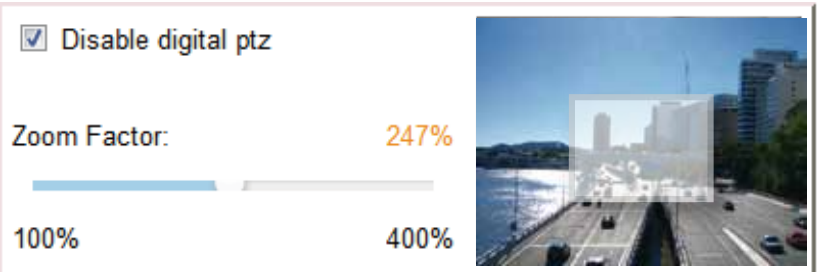
Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > General settings on page 46. The zoom ratio is also displayed with the title bar.

2.0x Title 2014/03/05 10:39:08

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and deselect the "Disable digital zoom" to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Pause: Pause the transmission of the streaming media. The button becomes the Resume button after clicking the Pause button.

Stop: Stop the transmission of the streaming media. Click the Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 31 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.

Mute: Turn off the Mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:

Video Title: The video title can be configured. For more information, please refer to Media > Image on page 46.

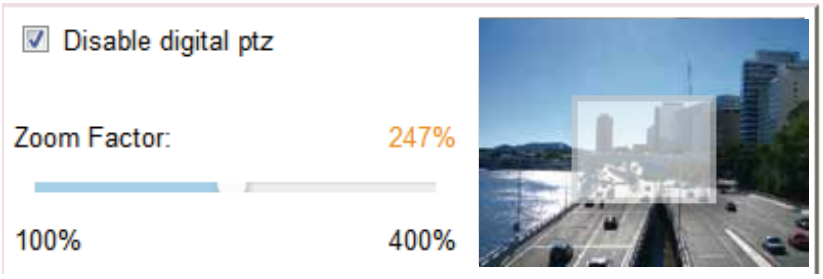
Time: Display the current time. For more information, please refer to Media > Image on page 46.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 46.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



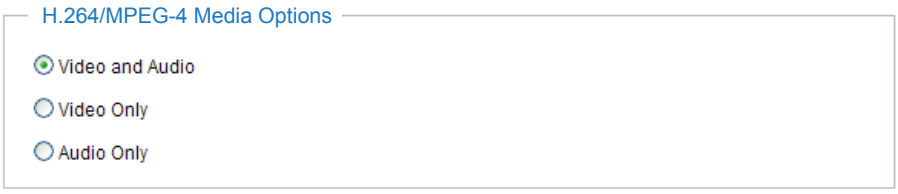
Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 31 for details.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

H.264/MPEG-4 Media Options



Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264 or MPEG-4.

H.264/MPEG-4 Protocol Options

Depending on your network environment, there are four transmission modes of H.264 or MPEG-4 streaming:

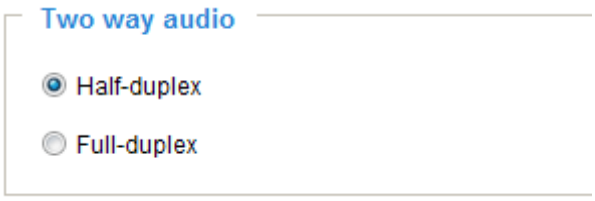
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 70.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

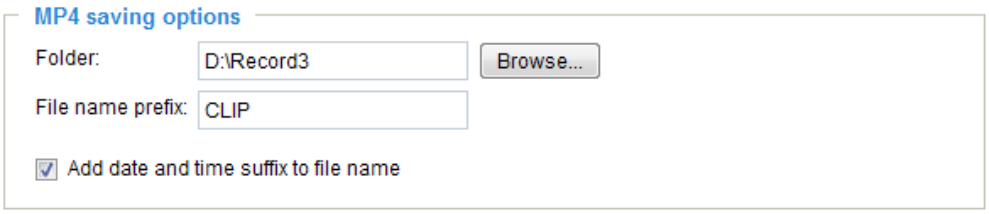
HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

Two way audio



Half duplex: Audio is transmitted from one direction at a time, e.g., from a PC holding a web console with the camera.
Full duplex: Audio is transmitted in both directions simultaneously.

MP4 Saving Options

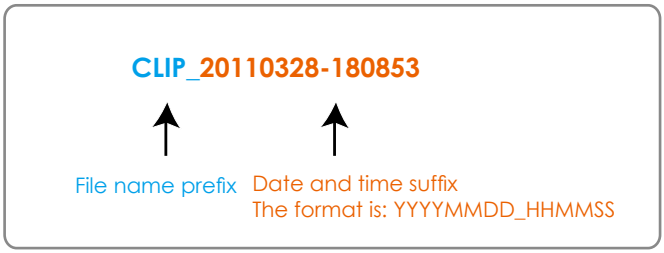


Users can record live video as they are watching it by clicking the button - Start MP4 Recording - on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

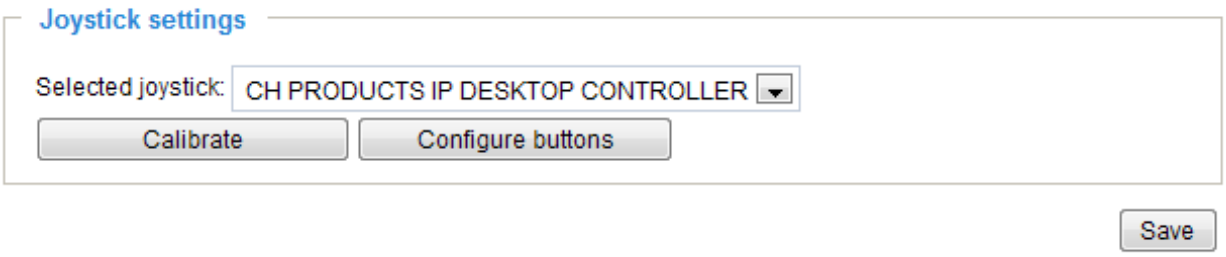
Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name of the recorded videos.



Local Streaming Buffer Time

In a busy network, fluctuations in available bandwidth can occur. Video streaming may lag and may not proceed very smoothly. If you enable this option, video streams from the camera will be temporarily stored on the computer's cache memory for a configurable period of time (seconds or milliseconds) before being played on a web session. This will help you see the streaming more smoothly. If you enter 3,000 Millisecond, the streaming will delay for 3 seconds.

Joystick Settings

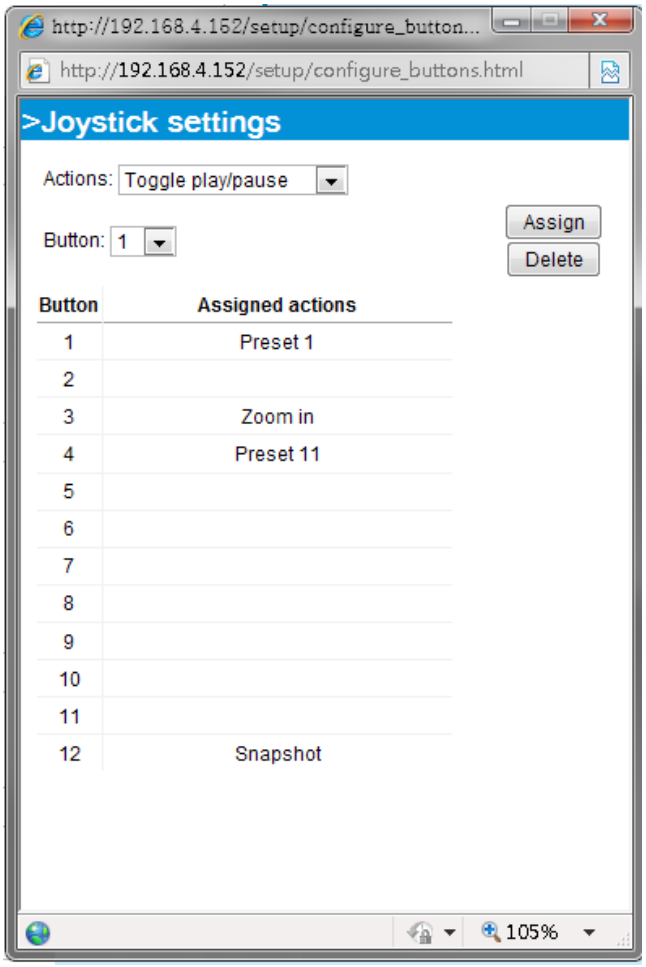


Enable Joystick

Connect to the USB plug of the joystick to a USB port on your management computer. Once a USB joystick is connected, the related joystick configuration will be available on the Client settings window. The joystick should work properly without installing any other driver or software.

Then you can begin to configure the joystick settings of connected devices. Please follow the instructions below to enable joystick settings.

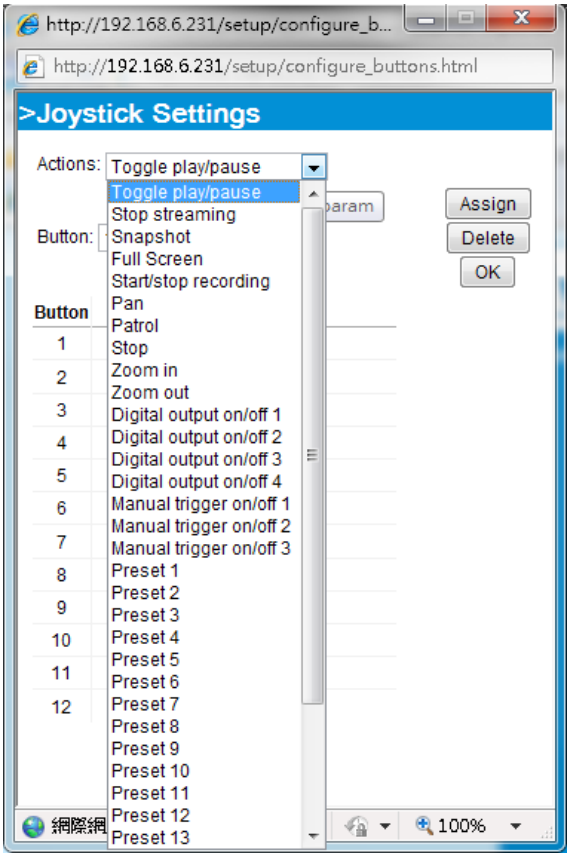
1. Click on the Configure buttons button. If your joystick is working properly, it will be displayed on the drop-down list.



Buttons Configuration

In the Joystick Settings window, you can use the combinations of pull-down menus, Actions and Button number, to assign joystick buttons with different functions. The number of buttons may differ from the joystick you attached.
Please follow the steps below to configure your joystick buttons:

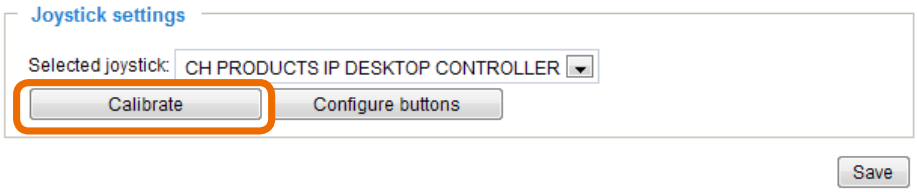
1. Select the number of the button you want to configure from its pull-down list.
   For example: Assign **Preset 1** (move to preset 1 position) to Button 1.



2. Select an action from the Actions menu. Click **Assign** to associate the button with an action.
3. Your configuration will be automatically saved.
4. To disable an assignment, select the number of a button, and then click the Delete button. The associated action will then be cleared.
5. Repeat the above process to assign actions to other buttons. When done, simply close the configuration window.

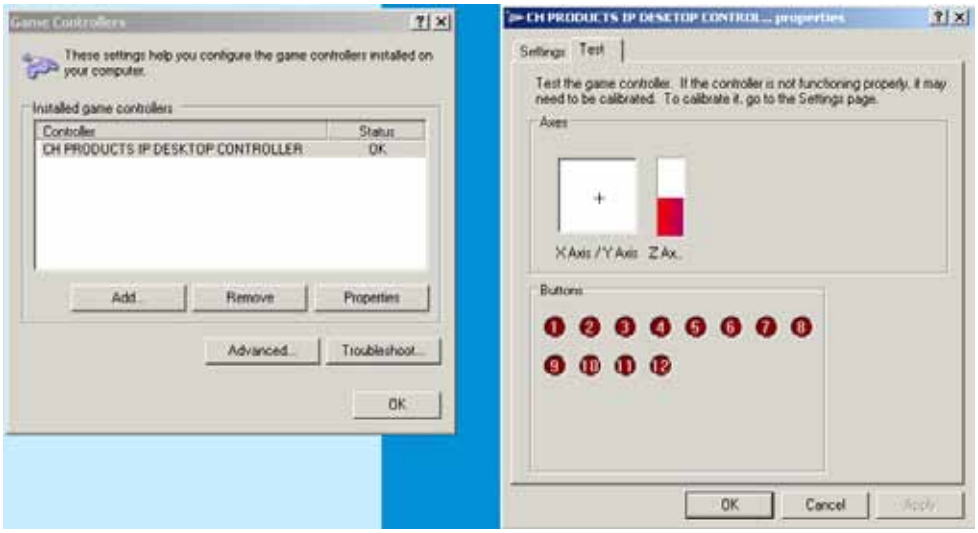
NOTE:

- If you want to assign Preset actions to your joystick, the PTZ preset locations should be configured in advance.
- If your joystick is not working properly, it may need to be calibrated. Click the Calibrate button to open the Game Controllers window located in Microsoft Windows control panel and follow the instructions for trouble shooting.



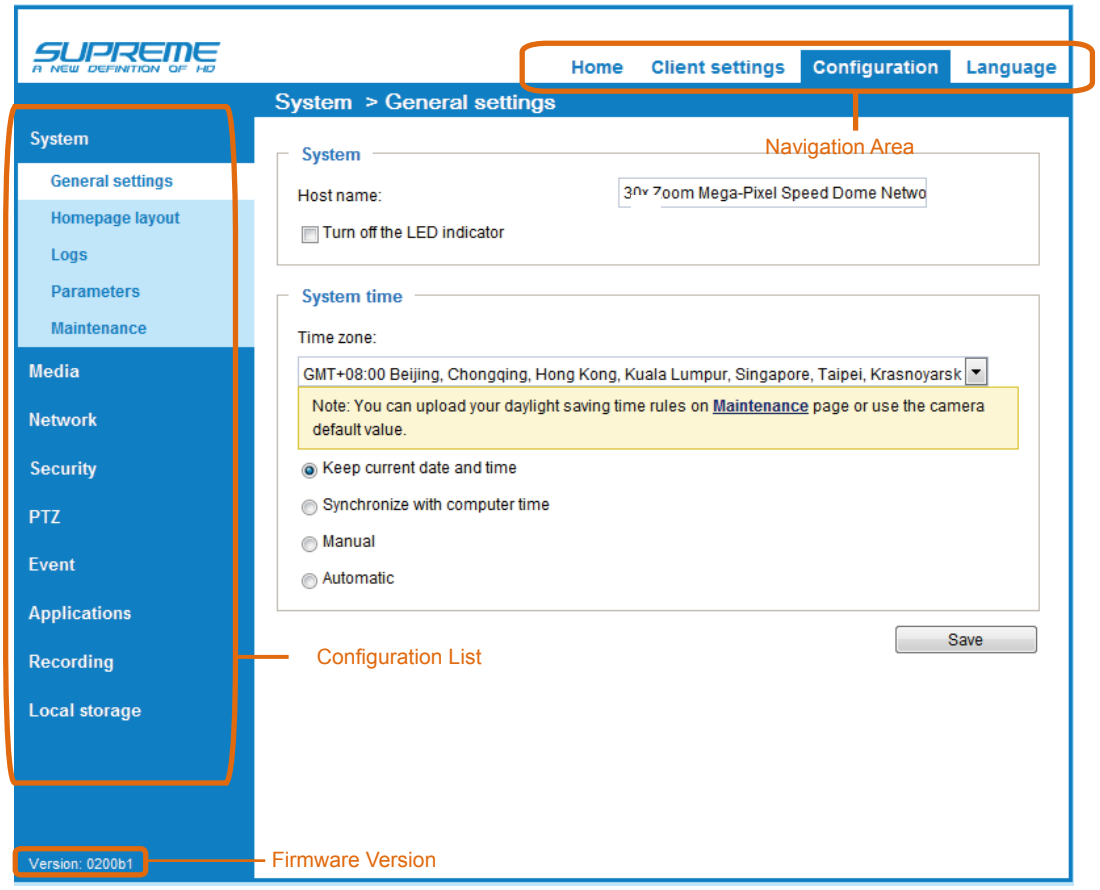
- The joystick will appear in the Game Controllers list in the Windows Control panel. If you want to check out for your devices, go to the following page: **Start** -> **Control Panel** -> **Game Controllers**.

- Follow the onscreen instructions to calibrate your joystick.



Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page. Please refer to page 78 Security > User Account for how to configure access rights for different users.



Each function on the configuration list will be explained in the following sections.

Navigation Area provides an instant switch among **Home** page (the monitoring page for live viewing), **Configuration** page, and multi-language selection.

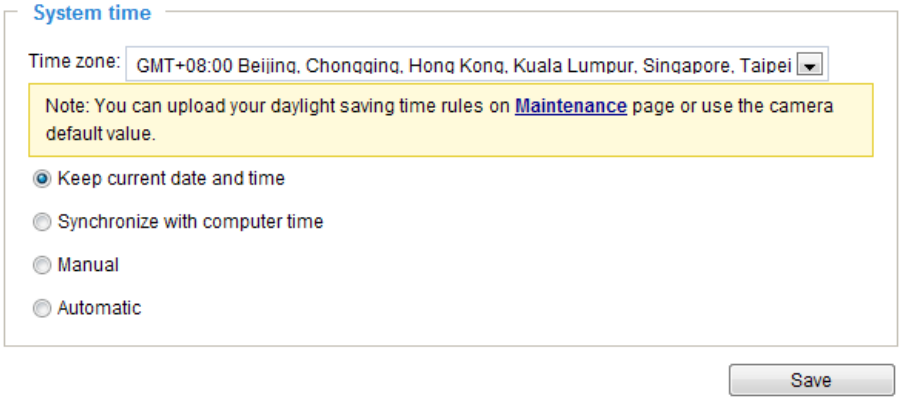
System > General settings

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following two columns: System and System Time.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page.

System time


System time
Time zone:
GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei
Note: You can upload your daylight saving time rules on Maintenance page or use the camera default value.
Keep current date and time
Synchronize with computer time
Manual
Automatic
Save

Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Synchronize with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of an established time server. Leaving the text box blank connects the Network Camera to the default time servers. The precondition is that your camera must have access to the Internet.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone : Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 43 for details.

When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System > Homepage layout

This section explains how to set up your own customized homepage layout.

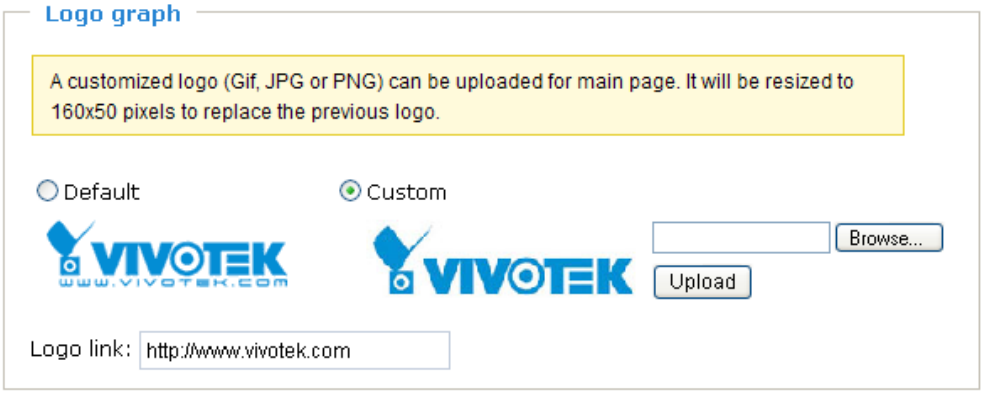
General settings

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the second tab on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

■ Hide Powered by VIVOTEK: If you check this item, such wording will be removed from the homepage.

Logo graph

Here you can change the logo at the top of your homepage.



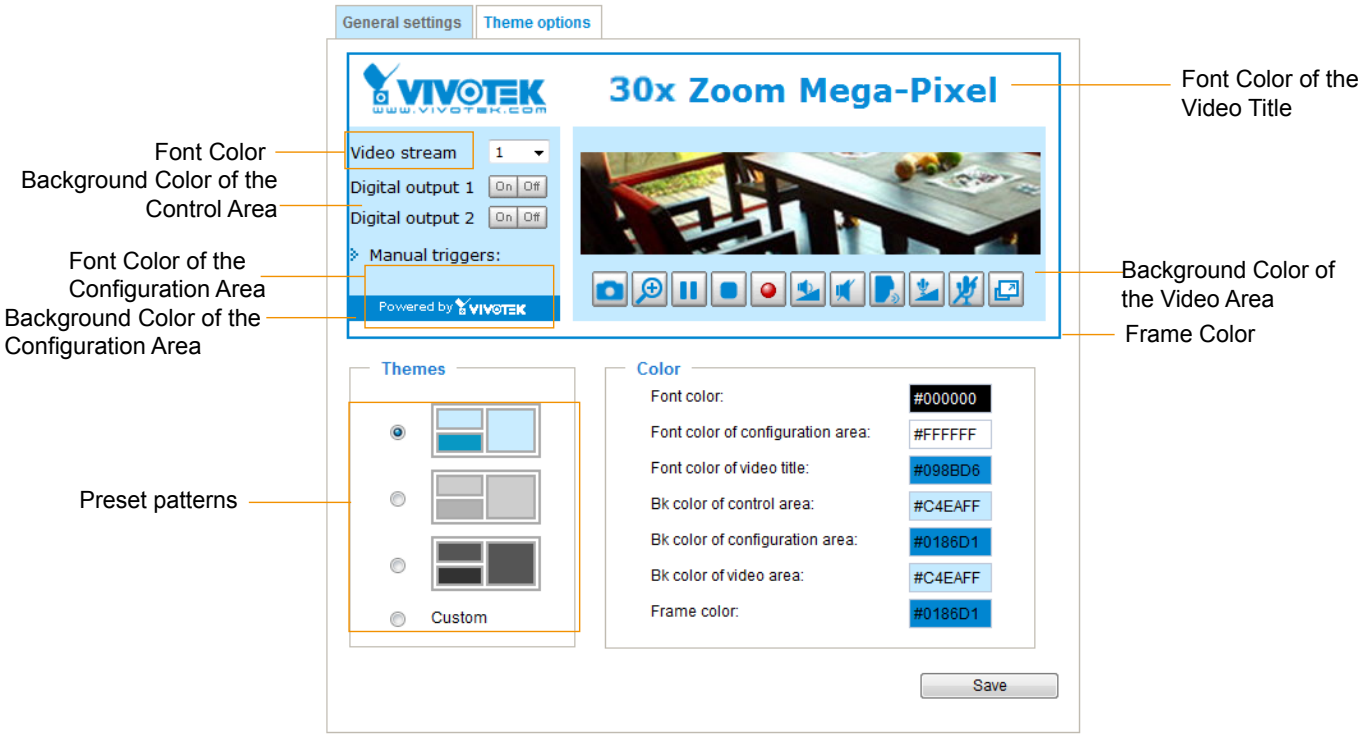
Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

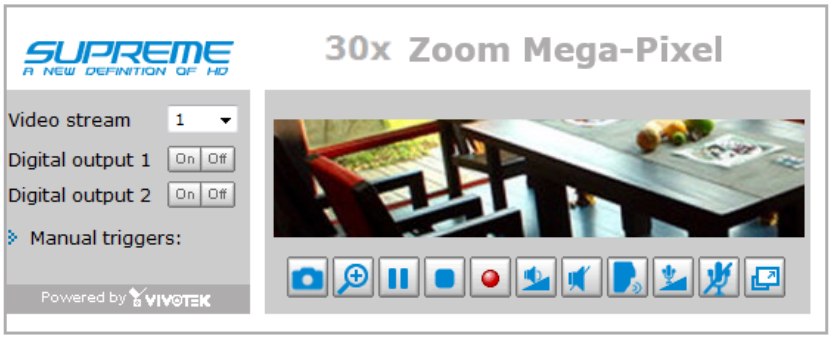
Customized button

Deselect the checkbox if you do not need the Manual trigger buttons on the main page.

Theme Options

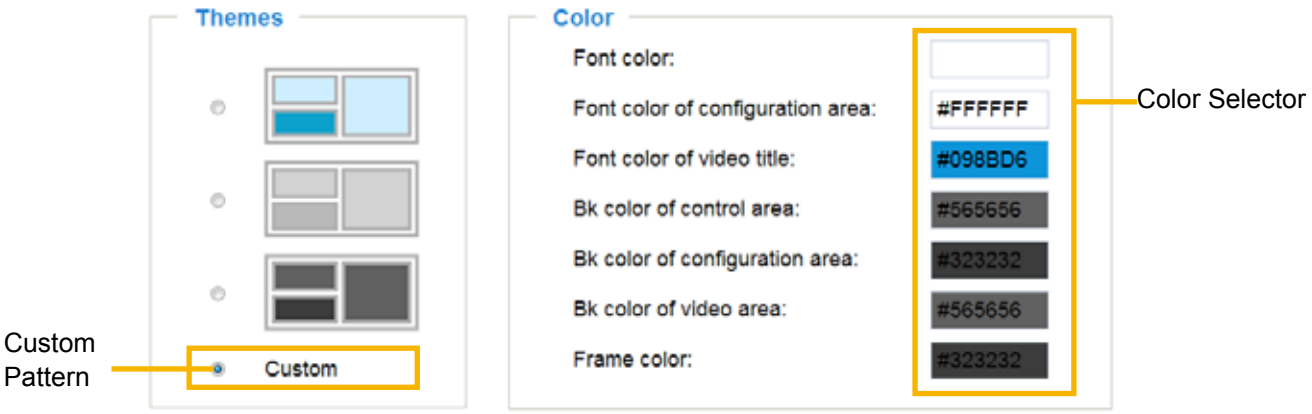
Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.



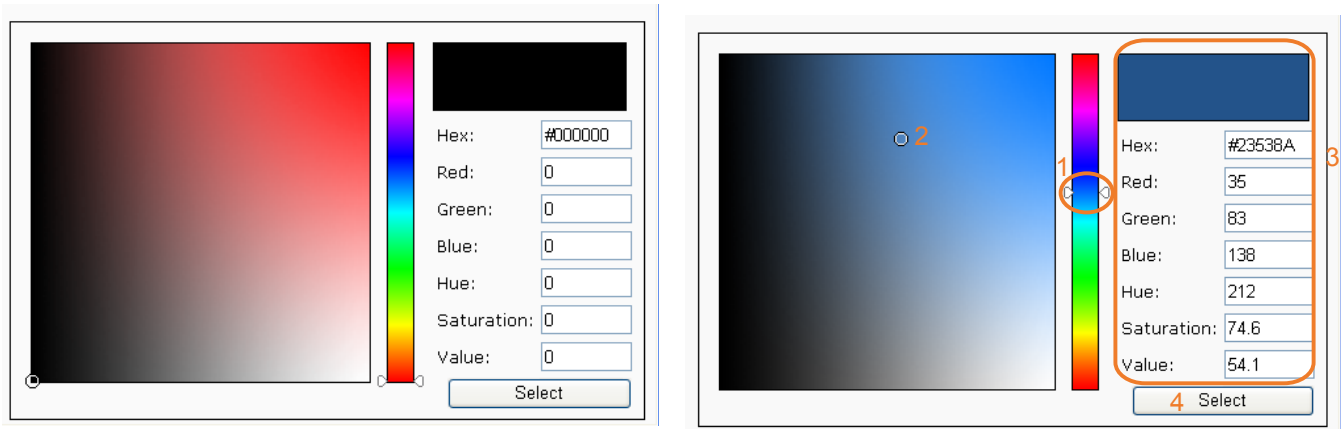


■ Follow the steps below to set up the customed homepage:

1. Click **Custom** on the left column.
2. A double-click on the color selection area (the right hand side column) will bring up a color palette window.

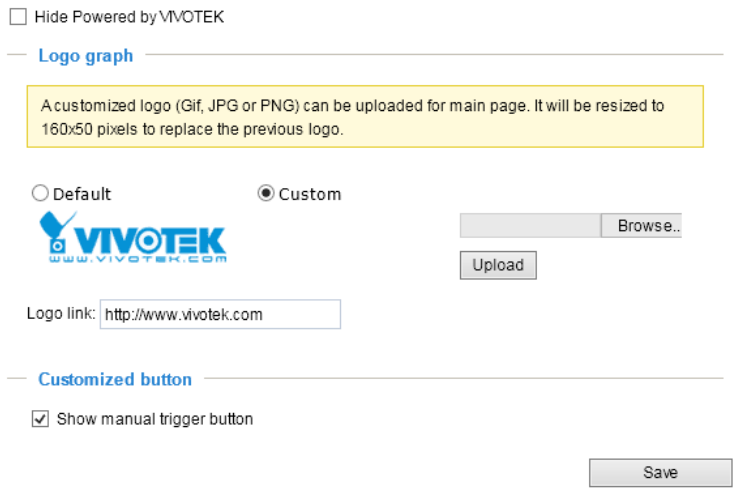


3. The palette window will pop up as shown below.



4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

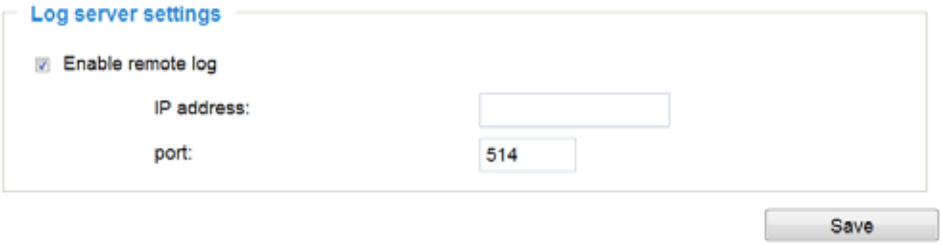
Below are the options for system integrators or VARs. You can use the checkboxes to replace VIVOTEK's company logo, the embedded website address or the slogan "Powered by VIVOTEK." When done, use the Save button to complete the configuration.



System > Logs

This section explains how to configure the Network Camera to send the system log to the remote server as backup.

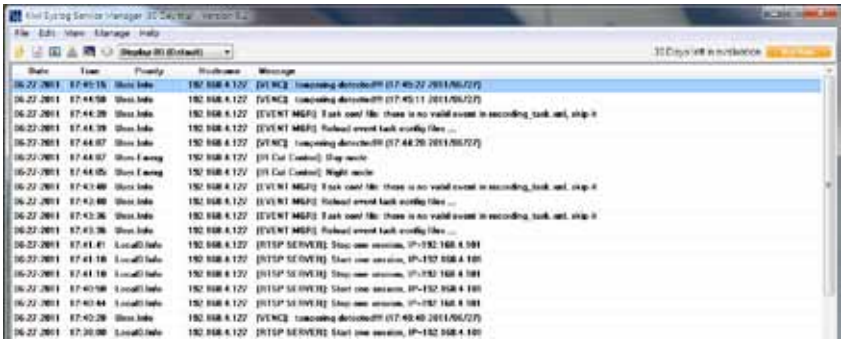
Log server settings



Follow the steps below to set up the remote log:

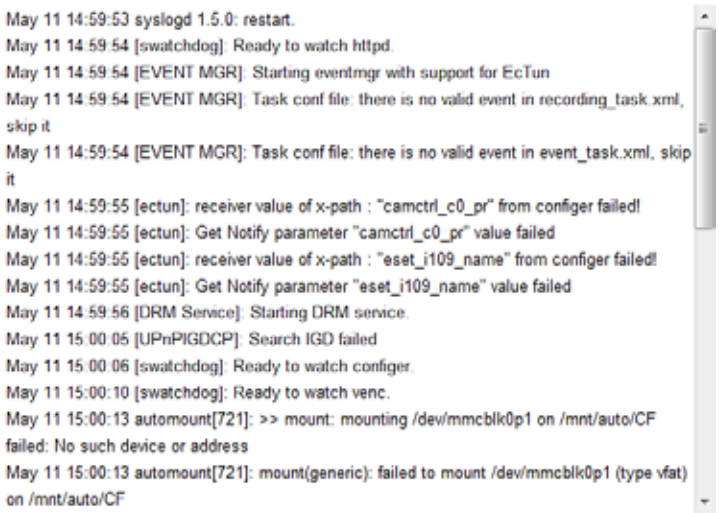
1. Select **Enable remote log**.
2. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, click **Save** to enable the setting.

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.



System log

This column displays the system log in a chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when the number of events reaches a preset limit.


May 11 14:59:53 syslogd 1.5.0: restart.
May 11 14:59:54 [swatchdog]: Ready to watch httpd.
May 11 14:59:54 [EVENT MGR]: Starting eventmgr with support for EcTun
May 11 14:59:54 [EVENT MGR]: Task conf file: there is no valid event in recording_task.xml, skip it
May 11 14:59:54 [EVENT MGR]: Task conf file: there is no valid event in event_task.xml, skip it
May 11 14:59:55 [ectun]: receiver value of x-path : "camctrl_c0_pr" from configer failed!
May 11 14:59:55 [ectun]: Get Notify parameter "camctrl_c0_pr" value failed
May 11 14:59:55 [ectun]: receiver value of x-path : "eset_i109_name" from configer failed!
May 11 14:59:55 [ectun]: Get Notify parameter "eset_i109_name" value failed
May 11 14:59:56 [DRM Service]: Starting DRM service.
May 11 15:00:05 [UPnPIGDCP]: Search IGD failed
May 11 15:00:06 [swatchdog]: Ready to watch configer.
May 11 15:00:10 [swatchdog]: Ready to watch venc.
May 11 15:00:13 automount[721]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or address
May 11 15:00:13 automount[721]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF

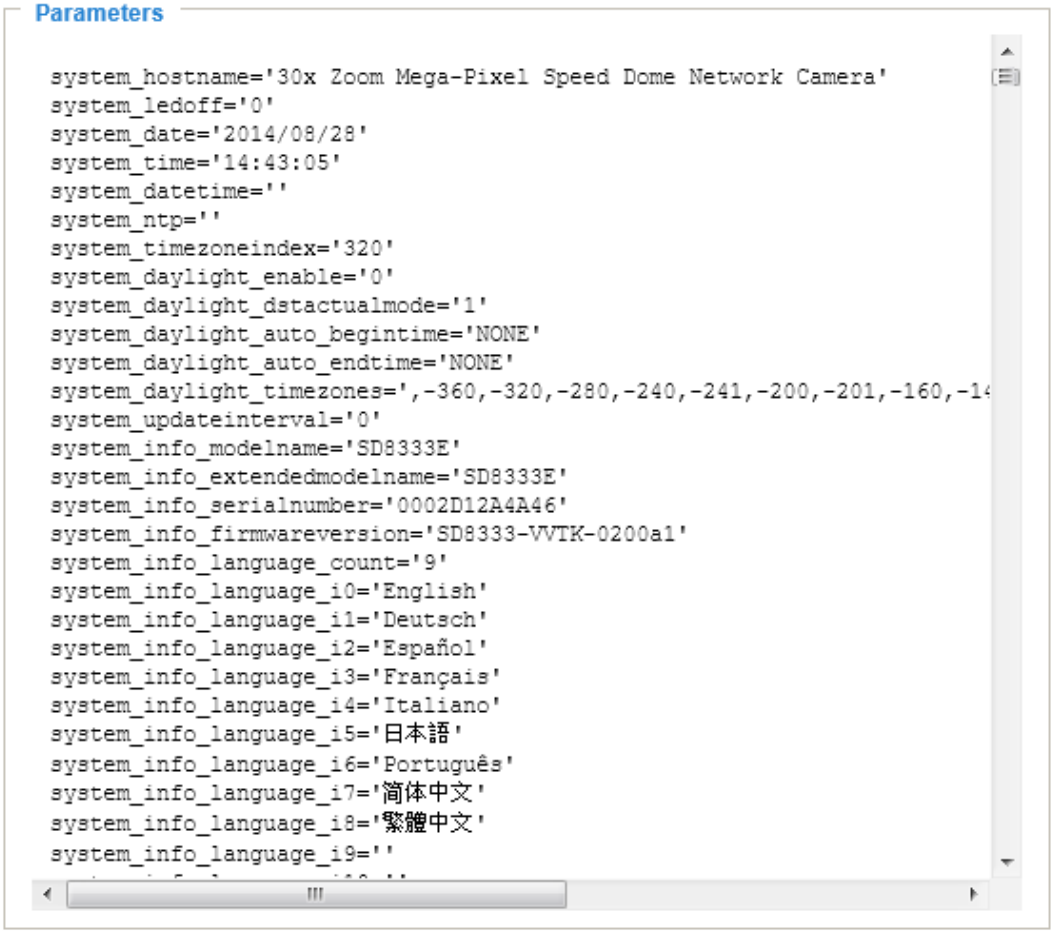
Access log

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

System log
Access log
Mar 9 15:54:25 [RTSP SERVER]: Start one session, IP=192.168.4.116
Mar 9 15:54:38 [RTSP SERVER]: Start one session, IP=192.168.4.116
Mar 9 15:58:16 [RTSP SERVER]: Stop one session, IP=192.168.4.116
Mar 9 15:58:18 [RTSP SERVER]: Start one session, IP=192.168.4.116
Mar 9 16:46:11 [RTSP SERVER]: Stop one session, IP=192.168.4.116
Mar 9 16:49:02 [RTSP SERVER]: Start one session, IP=192.168.4.116

System > Parameters

The View Parameters page lists the entire system's parameters in an alphabetical order. If you need technical assistance, please provide the information listed on this page.



System > Maintenance

This chapter explains how to restore the Network Camera to factory default, reboot, upgrade firmware version, etc.

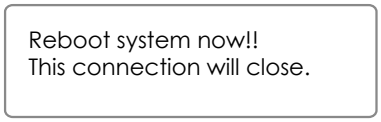
General settings > Upgrade firmware

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do not power off the Network Camera during the upgrade!

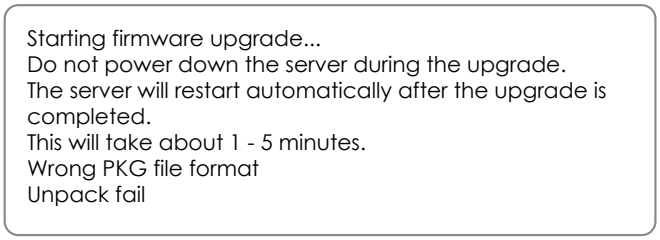
Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, refresh the management session with the Network Camera.

The following message is displayed when the upgrade has succeeded.

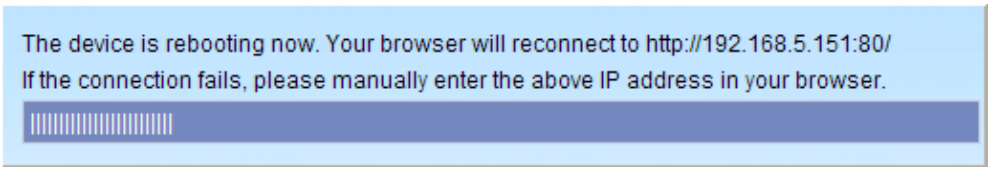


The following message is displayed when you have selected an incorrect firmware file.


Starting firmware upgrade...
Do not power down the server during the upgrade.
The server will restart automatically after the upgrade is completed.
This will take about 1 - 5 minutes.
Wrong PKG file format
Unpack fail

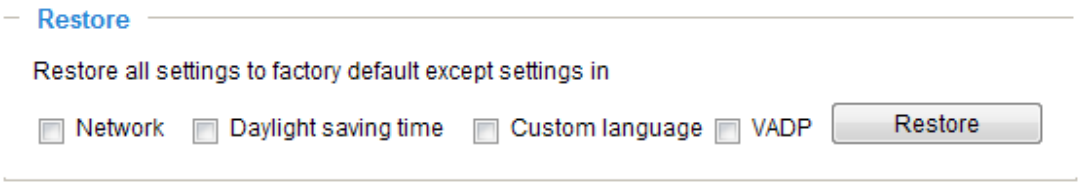
General settings > Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.


The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

General settings > Restore



This feature allows you to restore the Network Camera's factory defaults.

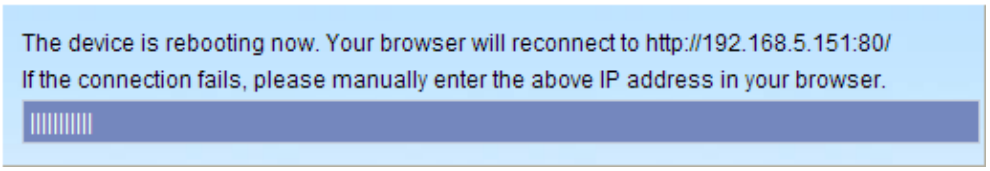
Network: Select this option to retain the Network Type settings (please refer to Network Type on page 60).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to Import/Export files below on this page).

Custom Language: Select this option to retain the Custom Language settings.

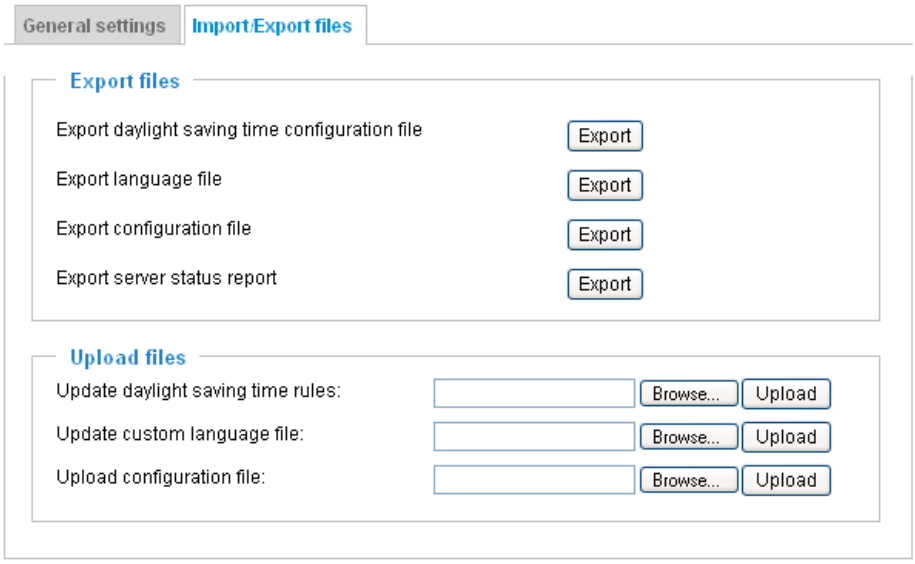
VADP: Retain the VADP modules (3rd-party software stored on the SD card) and related settings.

If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.


The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/
If the connection fails, please manually enter the above IP address in your browser.

Import/Export files

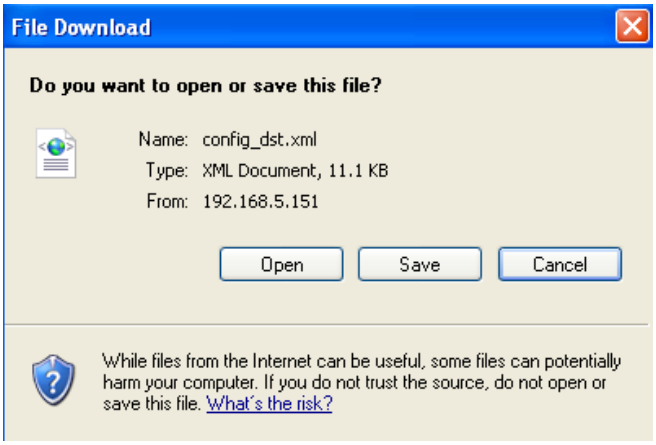
This feature allows you to Export / Update daylight saving time rules, custom language file, and configuration file.



Export daylight saving time configuration file: Click to set the start and end time of DST.

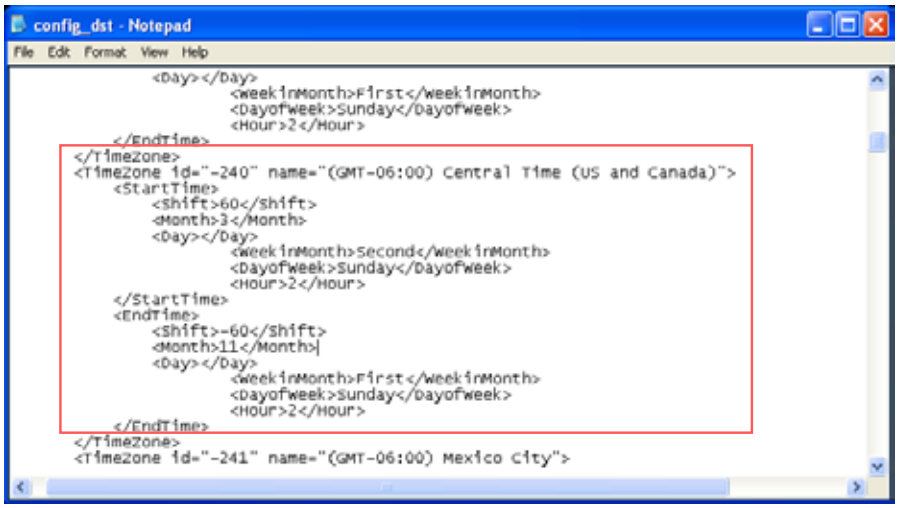
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.


File Download
Do you want to open or save this file?
Name: config_dst.xml
Type: XML Document, 11.1 KB
From: 192.168.5.151
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

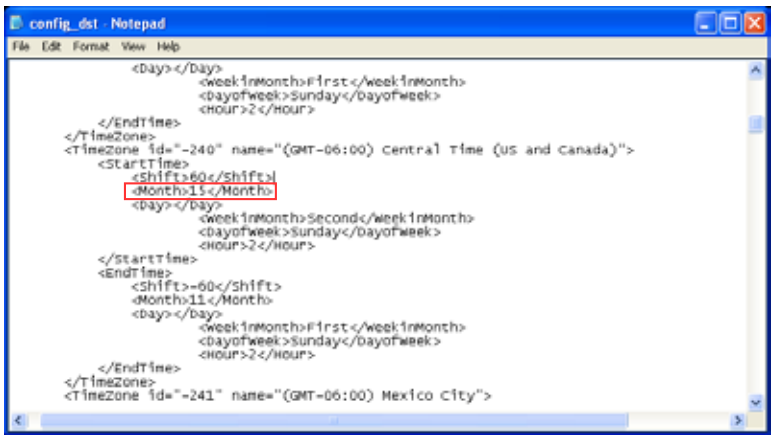
3. Open and edit the file using Microsoft® Notepad and locate your time zone in the strings; set the start and end time of DST. When completed, save the file.

   In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.

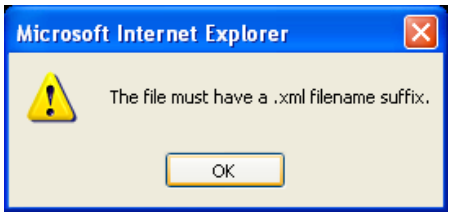


Update daylight saving time rules: Click **Browse…** and specify the XML file to update.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.



The following message is displayed when attempting to upload an incorrect file format.



Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Update custom language file: Click **Browse…** and specify your own custom language file to upload.

Export configuration file: Click to export all parameters for the device and user-defined scripts.

Update configuration file: Click **Browse…** to update a configuration file. Please note that the model and firmware version of the device should be identical to those specified for the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

Export server status report: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message..., and so on.

Tips:

- If a firmware upgrade is accidentally disrupted, say, by a power outage, you still have a last resort method to restore normal operation. See the following for how to bring the camera back to work:

  Applicable scenario:

  (1) Power disconnected during firmware upgrade.
  (2) Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

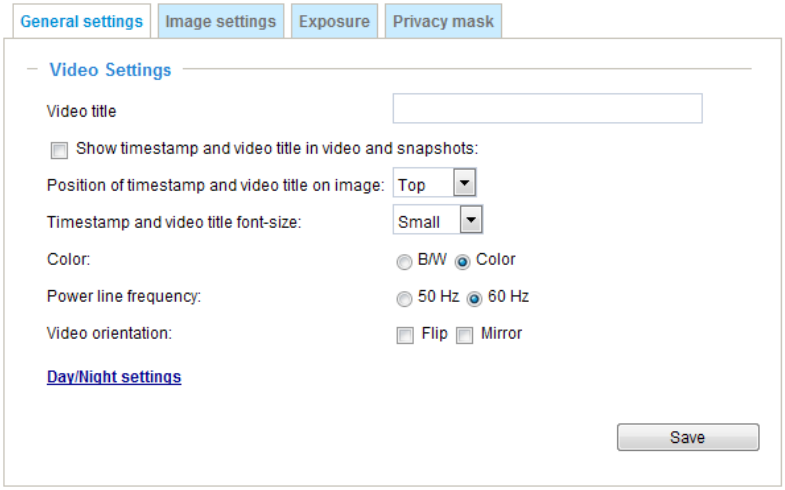
  You can use the following methods to activate the camera with its backup firmware:

  (1) Press and hold down the reset button for at least one minute.
  (2) Power on the camera until the Red LED blinks rapidly.
  (3) After boot up, the firmware should return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process). When this process is completed, the LED status should return to normal.

Media > Image

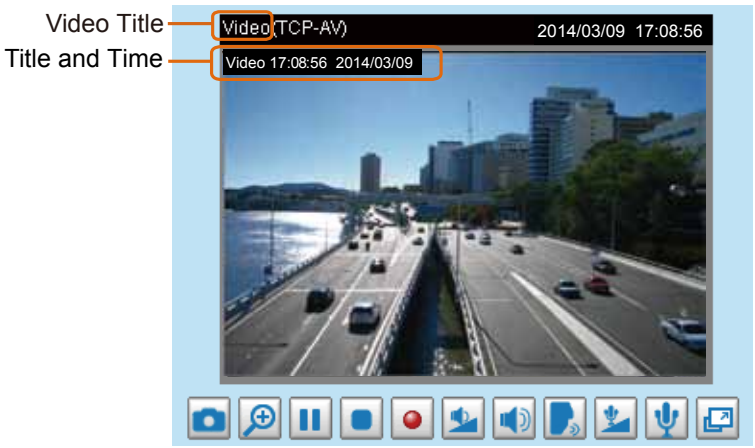
This section explains how to configure the image settings of the Network Camera. It is composed of the following four columns: General settings, Picture settings, Exposure, and Privacy mask.

General settings



Video title

Show_timestamp and video title in videos_and_snapshots: Enter a name that will be displayed on the title bar of the live video as the picture shown below.



Position of timestamp and video title on image: Select to display time stamp and video title on the top or at the bottom of the video stream.

Timestamp and video title font size: Select the font size for the time stamp and title.

Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

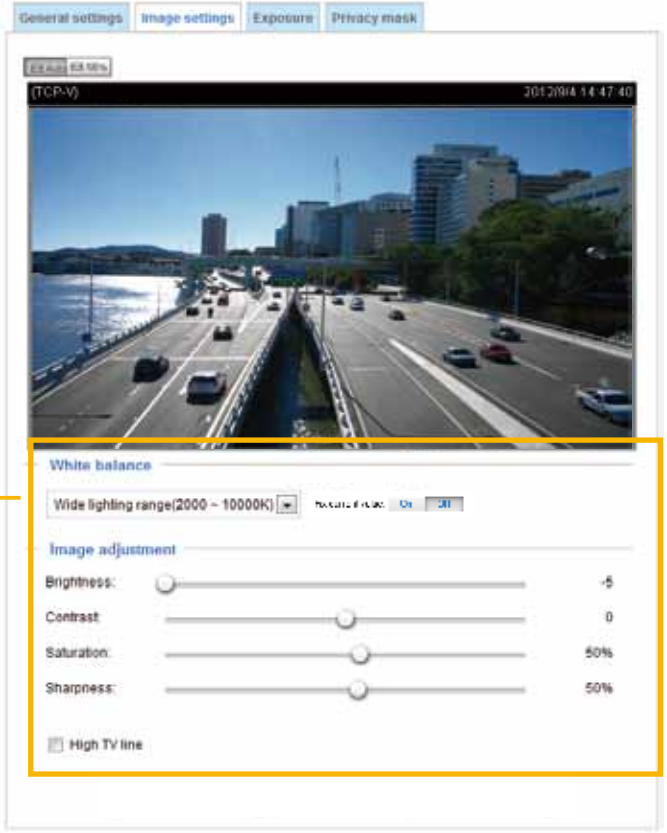
Video orientation: Flip - vertically reflect the display of the live video; Mirror - horizontally reflect the display of the live video. Change the settings if the Network Camera is installed in a different orientation (which is rare for a speed dome) to correct the image orientation.

Day/Night settings: This is a hyperlink to the Exposure > Day/Night setting page.

Image settings

On this page, you can tune the White balance and Image adjustment settings.

Sensor Setting 1:
For normal situations



White balance: Adjust the value for the best color temperature.

■ Select one of the white balance modes:

1. **Outdoor** (system default): Using this mode enables the camera to capture images with natural white balance observable in the morning.
2. **Fluorescent light**: 3,200K base mode, suitable for indoor applications.
3. **Wide lighting range**: This mode adapts to light temperatures ranging from 2,000 to 10,000K. This mode especially applies in areas where the camera needs to cover both indoor and outdoor areas.
4. **Sodium vapor lamp**: This mode applies to streets and highway lit by sodium vapor lamps.

■ Fix current value: This option is available when the Wide lighting range is selected. When selected, the camera will use the current color temperature setting. Note that you should use the Save button below to preserve current configuration. Otherwise, the white balance mode will return to Auto after you leave the configuration page.

■ Manual: In the manual mode, you can manually tune the R gain and Blue gain values by dragging the slide bars. Index numbers will be shown on the right hand side while changes in image is immediately displayed.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from -5 to +5.

■ Contrast: Adjust the image contrast level, which ranges from -5 to +5.

■ Saturation: Adjust the image saturation level, which ranges from 0% to 100%.

■ Sharpness: Adjust the image sharpness level, which ranges from 0% to 100%.

■ High TV line: This enhances the clarity of imaging details with high acutance. While the image quality is improved, noises may also increase at the same time.

Electronic image stabilizer

Select the checkbox to enable the Electronic image stabilization (EIS) function.

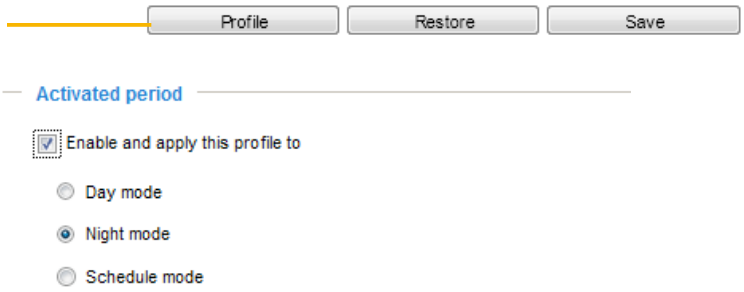
Enable 3D Noise reduction

- Check to enable noise reduction in order to reduce noises and flickers in image. This applies to the onboard 3D Noise Reduction feature. Use the pull-down menu to adjust the reduction strength. Note that applying this function to the video channel will consume system computing power.

  3D Noise Reduction is mostly applied in low-light conditions. When enabled in a low-light condition with fast moving objects, trails of after-images may occur. You may then select a lower strength level or disable the function.

Note that the **Preview** button has been cancelled, all changes made to image settings is directly shown on screen. You can click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting. You can also click on **Profile** to adjust all settings above in a pop-up window for special lighting conditions during a specific period of time in a day.

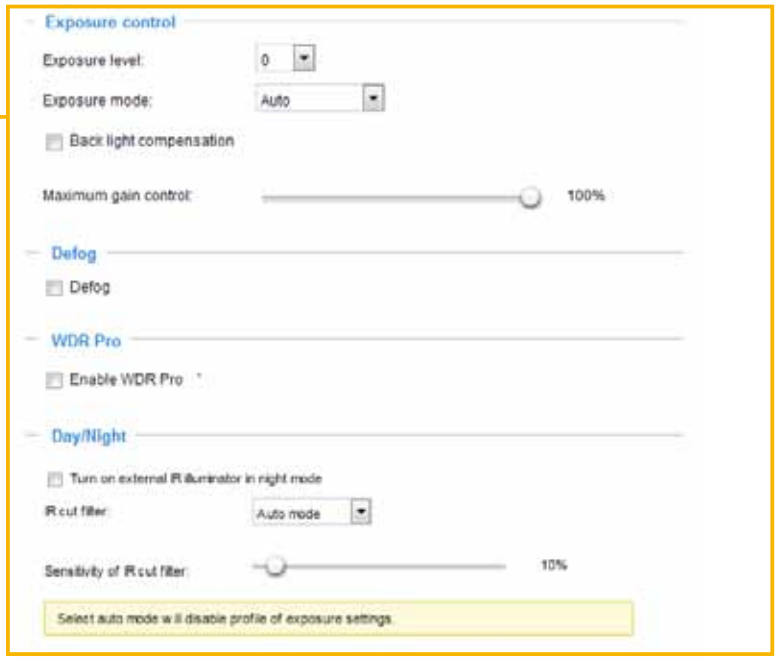
Sensor Setting 2:
For customized situations such as night mode.



Exposure

On this page, you can set the Exposure level, Max gain,Exposure mode, and IR cut filter related settings. Detailed configurations will be automatically adjusted since the sensor library will automatically adjust the value according to the ambient light.

Sensor Setting 1:
For normal situations



Sensor Setting 2:
For special situations

Exposure control:

■ **Exposure level**: You can manually set the Exposure level, which ranges from -2.0 to +2.0 (dark to bright). You can also select other values from the Exposure mode menus and select a preferred scenario or manually configure the associated settings. You may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.

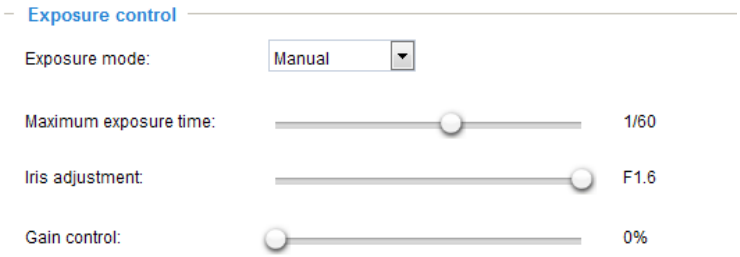
■ **Exposure mode**:

Select **Auto, Shutter Priority, Iris Priority,** or **Manual** mode according to your needs.
- Auto: System default, which automatically adjusts the iris, shutter speed, and gain for an optimmal exposure level.

- Shutter Priority: When selected, the **Exposure time** slide bar will appear, allowing you to select an exposure time ranging from 1/10,000, to 1/1 second. Once a fixed value is selected, system firmware will automatically tune the gain and iris settings to match an optimal exposure level.

- Iris Priority: When selected, the **Iris adjustment** slide bar will appear, allowing you to select an aperture size ranging from F14 to F1.6. Once a fixed value is selected, system firmware will automatically tune the gain and exposure time to match an optimal exposure level. The value is measured in the F-number as the ratio of the focal length to the lens diameter. Iris size is inversely proportional to the F-number; therefore, the smaller the F-number, the greater is the exposure ratio. Smaller F-number (larger exposure ratio, largest size of lens aperture opening) is shown on the right of the slide bar.

- Manual: Select **Manual** to set a fixed exposure time, iris, and gain. Then, tune the slide bar to set the Exposure time, Iris adjustment, and Gain Control to the best image quality. A shorter exposure time allows less amount of light to enter the sensor; while a higher gain control value generates certain amount of noises.

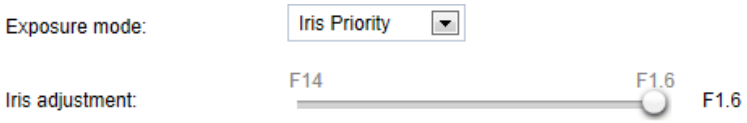


Note the following when the **Manual** mode is selected:
1. The **Exposure level** bar will not be available.
2. The **IR cut filter** setting will switch to **Day Mode**. If it was previously configured into other modes, the previous setting remains intact.

Manual: (**Note that some of the Manual options will be disabled when WDR Pro is enabled!**)

NOTE:

- When **Iris Priority** is selected for the **Exposure mode**, the tunable aperture size is related to zoom ratio. When using different zoom ratios, the range of aperture sizes can be different. When zoom ratio is 0x, the range of iris sizes is F1.6~F14. When zoom ratio is 20x, the iris size is F3.4. See below for the corresponding maximum iris sizes at different zoom ratios:



Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.
1.00	1.4	1.14	1.6	1.28	1.8	1.42	1.9	1.56	2.1	1.70	2.2	1.84	2.2	1.98	2.3
1.01	1.4	1.15	1.6	1.29	1.8	1.43	1.9	1.57	2.1	1.71	2.2	1.85	2.3	1.99	2.3
1.02	1.4	1.16	1.6	1.30	1.8	1.44	2.0	1.58	2.1	1.72	2.2	1.86	2.3	2.00	2.3
1.03	1.4	1.17	1.6	1.31	1.8	1.45	2.0	1.59	2.1	1.73	2.2	1.87	2.3	2.01	2.3
1.04	1.5	1.18	1.7	1.32	1.8	1.46	2.0	1.60	2.1	1.74	2.2	1.88	2.3	2.02	2.3
1.05	1.5	1.19	1.7	1.33	1.8	1.47	2.0	1.61	2.1	1.75	2.2	1.89	2.3	2.03	2.4
1.06	1.5	1.20	1.7	1.34	1.9	1.48	2.0	1.62	2.1	1.76	2.2	1.90	2.3	2.04	2.4
1.07	1.5	1.21	1.7	1.35	1.9	1.49	2.0	1.63	2.1	1.77	2.2	1.91	2.2	2.05	2.4
1.08	1.5	1.22	1.7	1.36	1.9	1.50	2.0	1.64	2.1	1.78	2.2	1.92	2.3	2.06	2.4
1.09	1.5	1.23	1.7	1.37	1.9	1.51	2.0	1.65	2.1	1.79	2.2	1.93	2.3	2.07	2.4
1.10	1.5	1.24	1.7	1.38	1.9	1.52	2.0	1.66	2.1	1.80	2.2	1.94	2.3	2.08	2.4
1.11	1.6	1.25	1.8	1.39	1.9	1.53	2.0	1.67	2.1	1.81	2.2	1.95	2.3	2.09	2.4
1.12	1.6	1.26	1.8	1.40	1.9	1.54	2.0	1.68	2.1	1.82	2.2	1.96	2.3	2.10	2.4
1.13	1.6	1.27	1.8	1.41	1.9	1.55	2.1	1.69	2.2	1.83	2.2	1.97	2.3	2.11	2.4

Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.
2.12	2.3	2.26	2.5	2.40	2.5	2.54	2.6	2.68	2.6	2.82	2.6	2.96	2.7	3.36	2.8
2.13	2.4	2.27	2.5	2.41	2.5	2.55	2.6	2.69	2.6	2.83	2.6	2.97	2.7	3.40	2.8
2.14	2.4	2.28	2.5	2.42	2.5	2.56	2.6	2.70	2.6	2.84	2.6	2.98	2.7	3.44	2.8
2.15	2.4	2.29	2.5	2.43	2.5	2.57	2.6	2.71	2.6	2.85	2.7	2.99	2.7	3.49	2.8
2.16	2.4	2.30	2.5	2.44	2.5	2.58	2.6	2.72	2.6	2.86	2.7	3.00	2.7	3.53	2.8
2.17	2.3	2.31	2.5	2.45	2.5	2.59	2.6	2.73	2.6	2.87	2.7	3.01	2.7	3.58	2.8
2.18	2.4	2.32	2.5	2.46	2.5	2.60	2.6	2.74	2.6	2.88	2.7	3.05	2.7	3.62	2.8
2.19	2.4	2.33	2.5	2.47	2.5	2.61	2.6	2.75	2.6	2.89	2.7	3.09	2.7	3.67	2.8
2.20	2.3	2.34	2.5	2.48	2.5	2.62	2.6	2.76	2.6	2.90	2.7	3.12	2.7	3.72	2.9
2.21	2.4	2.35	2.5	2.49	2.5	2.63	2.6	2.77	2.6	2.91	2.7	3.16	2.7	3.76	2.9
2.22	2.4	2.36	2.5	2.50	2.6	2.64	2.6	2.78	2.6	2.92	2.7	3.20	2.7	3.81	2.9
2.23	2.5	2.37	2.5	2.51	2.6	2.65	2.6	2.79	2.6	2.93	2.7	3.24	2.8	3.86	2.9
2.24	2.5	2.38	2.5	2.52	2.6	2.66	2.6	2.80	2.6	2.94	2.7	3.28	2.8	3.92	2.9
2.25	2.5	2.39	2.5	2.53	2.6	2.67	2.6	2.81	2.6	2.95	2.7	3.32	2.8	3.97	2.9

Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.	Zoom ratio	F no.
4.02	2.9	4.89	3.1	6.05	3.2	7.59	3.3	9.64	3.5	12.28	3.5	15.66	3.4	20.76	3.4
4.08	2.9	4.96	3.1	6.14	3.2	7.72	3.4	9.80	3.5	12.49	3.5	15.94	3.4	21.29	3.4
4.13	2.9	5.04	3.1	6.24	3.2	7.85	3.4	9.98	3.5	12.71	3.5	16.23	3.4	21.85	3.4
4.19	2.9	5.11	3.1	6.34	3.2	7.98	3.4	10.15	3.5	12.93	3.5	16.53	3.4	22.47	3.4
4.25	3.0	5.19	3.1	6.44	3.2	8.12	3.4	10.33	3.5	13.15	3.5	16.84	3.4	23.15	3.4
4.30	3.0	5.26	3.1	6.55	3.3	8.26	3.4	10.51	3.5	13.38	3.5	17.16	3.4	23.89	3.4
4.36	3.0	5.34	3.1	6.65	3.3	8.40	3.4	10.69	3.5	13.61	3.5	17.49	3.4	24.72	3.5
4.43	3.0	5.43	3.1	6.76	3.3	8.54	3.4	10.88	3.5	13.85	3.5	17.83	3.4	25.66	3.5
4.49	3.0	5.51	3.1	6.87	3.3	8.69	3.4	11.07	3.5	14.09	3.5	18.19	3.4	26.74	3.6
4.55	3.0	5.59	3.1	6.99	3.3	8.84	3.4	11.26	3.5	14.34	3.5	18.56	3.4	28.00	3.7
4.62	3.0	5.68	3.2	7.10	3.3	8.99	3.4	11.46	3.5	14.59	3.5	18.96	3.4		
4.68	3.0	5.77	3.2	7.22	3.3	9.15	3.4	11.66	3.5	14.85	3.5	19.37	3.4		
4.75	3.0	5.86	3.2	7.34	3.3	9.31	3.4	11.86	3.5	15.11	3.5	19.80	3.4		
4.82	3.0	5.59	3.2	7.46	3.3	9.47	3.5	12.07	3.5	15.38	3.4	20.27	3.5		

- **Back light compensation**: This option is only available when the Auto mode is selected for the Exposure setting. This option enables light compensation for images that are too dark to recognize; for example, for the dark side of objects that is posed against bright sunlight. This option is disabled if you enable the WDR function.
- **Maximum gain control**: Select a maximum value for the electronic gain from the slide bar. The gain value also has its effect on the sensitivity of the IR cut filter. When applying the gain control, IR cut filter setting will change accordingly.
- **Defog**: This function allows you to configure post-image defog, which helps in a misty, raining weather.
- **WDR Pro (Wide Dynamic Range)**: Default is off. When set to Auto, you can select the strength of the WDR function. The Low, Medium, High options correspond to the level of contrast between the overly-lit area and the shaded areas. For example, the High option applies to a high contrast scenario. Note that when the exposure time is set to longer than 1/60 second, the WDR function will be disabled.

IMPORTANT:

1. **If you have different WDR settings in the normal and Profile settings, live view will also be temporarily disabled.**
2. **When the Electronic image stabilizer is enabled, the live view on the main page will zoom in slightly to a 1.1 ratio.**

Day/Night Settings

■ **Turn on external IR illuminator in night mode**
The camera's digital output signal can be connected to external IR lights to turn it on when the camera detects low light conditions and enters the night mode.

IR cut filter
With a removable IR-cut filter, this Network Camera can automatically remove the filter to let IR light enter the light sensor during low light conditions.

■ Auto mode
The Network Camera automatically removes the filter by judging the level of ambient light.

■ Day mode
In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.

■ Night mode
In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

■ Schedule mode
The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

IMPORTANT:

1. Because the exposure settings are also available in the **Profile** setting, incorrect configurations such as a very high exposure level will let the camera consider it is operating in the Day mode even when the ambient light is actually low. The camera will falsely remove the IR cut filter, and thus results in distorted image colors.

   Therefore, when the IR cut filter is in the Auto mode, the **Profile** setting is not available.
2. When set to the Night mode, the image display automatically changes to Black and White.
3. There is no Preview button in the Exposure window. Configuration changes are directly reflected in the live view window.

Exposure Profile: (Only available when the IR cut filter is not set to the Auto mode)

If you want to configure another sensor and exposure setting for an individual day/night/schedule mode, please click **Profile** to open the Profile of exposure settings page as shown below.

Activated period: Select the mode this profile to apply to: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode. Then check **Save** to take effect.

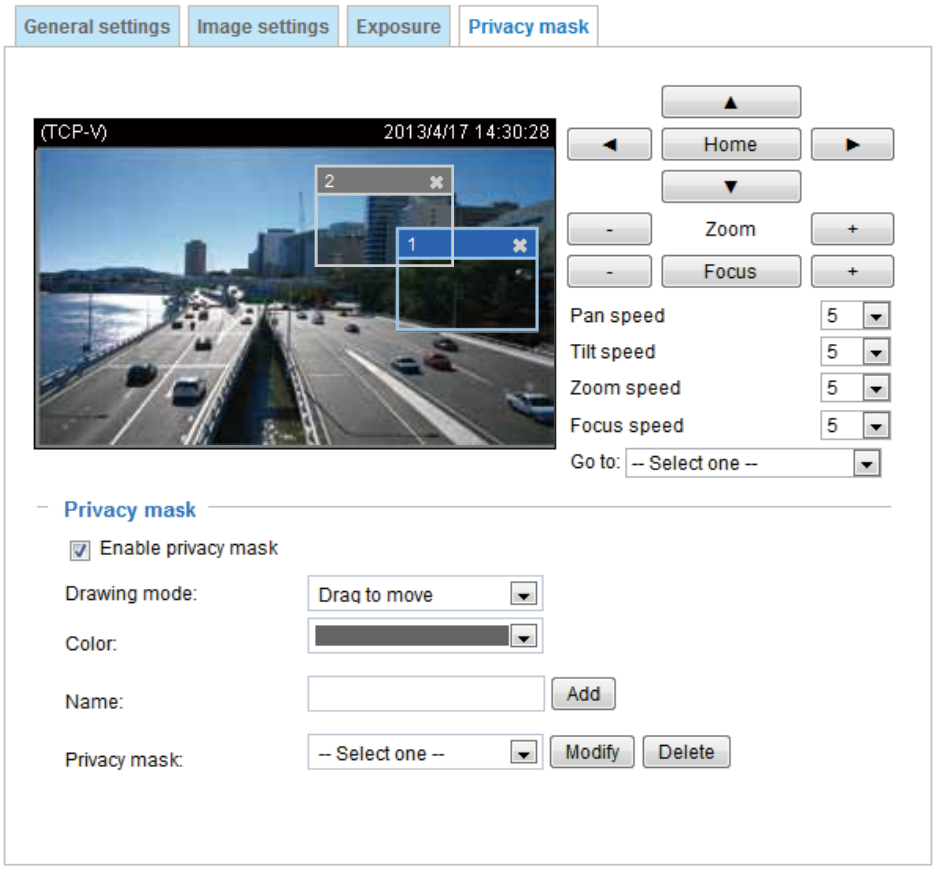
Please follow the steps below to set up a profile:

1. Check **Enable and apply this profile to**.
2. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode.

   When a span of time is configured using the Schedule mode, you can configure the Day/Night setting for controlling the behavior of the IR cut filter during that time.
3. Configure Exposure control settings in the folowing columns. Please refer to previous dicussions for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the window.

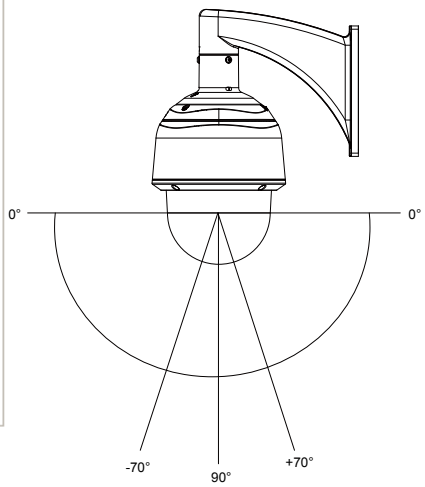
Privacy mask

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive view areas to address privacy concerns.



NOTE:

1. The navigation buttons here also support the continuous move. You can click and hold down the button to move across the screen until you release the button.
2. You can not create privacy masks at angles between +70° and -70°.



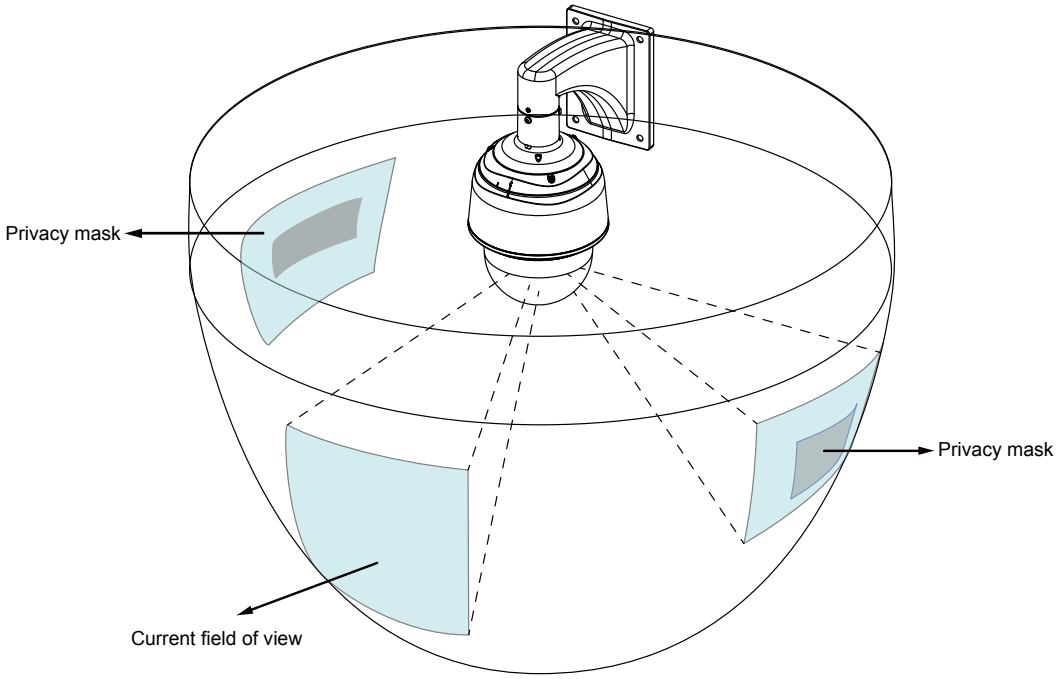
■ To set the privacy mask windows, follow the steps below:

1. Click on the **Enable privacy mask** checkbox to enable this function.
2. Use mouse clicks on the screen to move to a place where you want to create a mask. You can also use the PTZ panel to fine-tune the move to the target area.
3. Enter a name for the masking window. Click **Add** to create a new window.
4. Click on the **Modify** button and then use the mouse cursor to re-size the masking window, which is recommended to be at least twice the size of the object (height and width) you want to cover. You can select the Drawing mode as "Fixed in center" or "Drag to move."
   - When using the **Fixed in center** mode, you can move to the area of your interest, and then manually change the size and shape of the masking window.
   - When using the **Drag to move** mode, you can move to an area of your interest using the PTZ buttons above, and then click and drag to draw a masking window. The click to move maneuver is not available when you select the Drag to move mode.
5. You can also change the color of the mask from the **Color** menu.
6. If preferred, move the field of view to other places to create more privacy masks.

You may be prompted by the message when trying to create a privacy mask at angles between +70° and -70°.

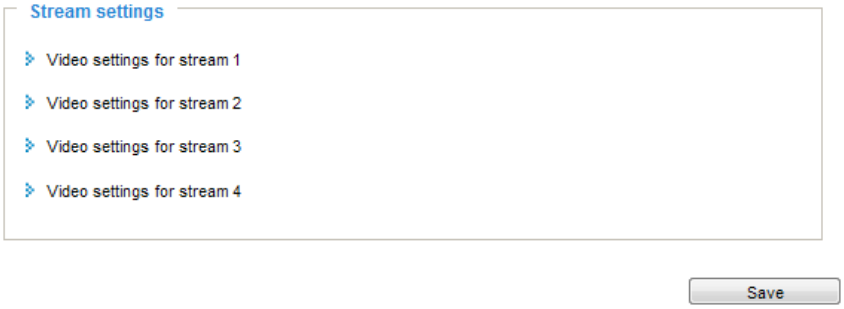
NOTE:

- The camera supports "**3D Privacy Mask**." Privacy masks should stay at the same positions regardless of how the camera lens may move.
- When the "Enabled privacy mask" checkbox is deselected, no privacy masks will appear on screen.
- Up to **24** privacy mask windows can be configured over the camera's hemispheric coverage.
- If you want to delete a privacy mask window, select its name from the pull-down menu at the bottom, and then click **Delete** to remove it.



Media > Video

Stream settings

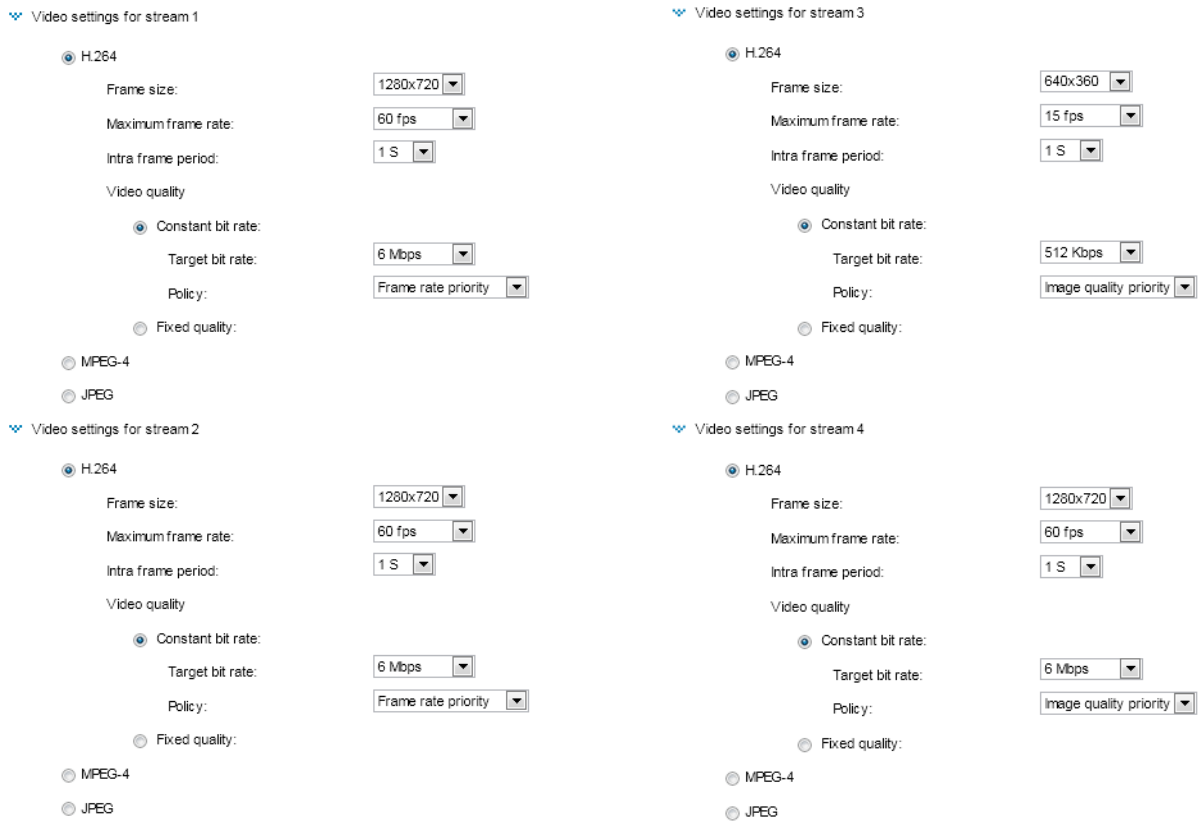


This Network Camera supports multiple streams with frame sizes ranging from 176 x 144 to 1280 x 720 pixels.

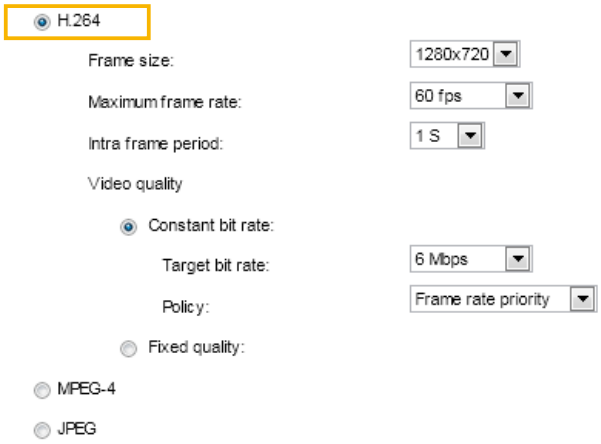
The definition of multiple streams:

- Stream 1: Users can define the Frame sizes, compression format, image quality, etc.
- Stream 2: The default frame size for stream 2 is configured to 1280 x 720.
- Stream 3: The default frame size for Stream 3 is set to the minimized 640 x 360 for viewing on mobile devices.
- Stream 4: The default frame size for stream 4 is configured to 1280 x 720 in the H.264 mode.

Click the stream item to display the detailed information. .



This Network Camera offers real-time H.264, MPEG-4, and MJPEG compression standards (Multiple Codec) for real-time viewing. If the **H.264 / MPEG-4** mode is selected, the video is streamed via RTSP protocol. There are several parameters through which you can adjust the video performance:



NOTE:

► *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*

► *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality and for recognizing moving objects in the field of view.

If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, 30fps, 40fps, 45fps, and 50fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, 30fps, 40fps, 45fps, 50fps, 55fps, and 60fps. You can also select **Customize** and manually enter a value.

■ Intra frame period
Determine how often for firmware to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality

Constant bit rate:

- Constant bit rate: A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, 8Mbps, 10Mbps, 12Mbps, 14Mbps, and 16Mbps. You can also select **Customize** and manually enter a value.

  - Target bit rate: Select a bit rate from the pull-down menu. The bit rate ranges from 20kbps to a maximum of 16Mbps. The bit rate then becomes the Average or Upper bound bit rate number. The Network Camera will strive to deliver video streams around or within the bit rate limitation you impose.

  - Policy: If Frame Rate Priority is selected, the Network Camera will try to maintain the frame rate per second performance, while image quality will sometimes be compromised. If Image quality priority is selected, the Network Camera may drop some video frames in order to maintain the image quality of individual frames.

- Fixed quality: On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

  - Maximum bit rate: With the fixed image quality, you can still impose an upper threshold on the maximum bit rate as a ceiling value. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gains.

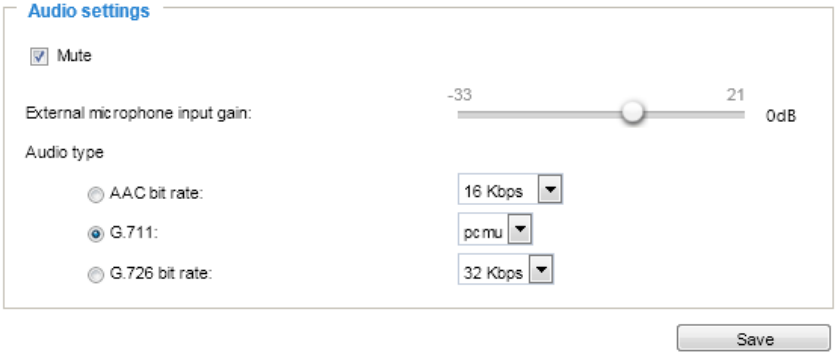
NOTE:

► *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*

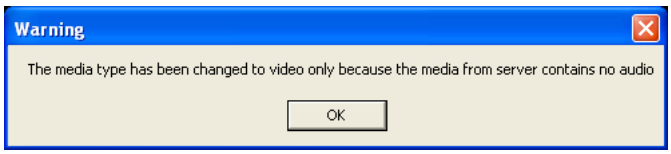
► *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurence, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Media > Audio

Audio Settings



Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if muted, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:



External microphone input gain: Select the gain of the external audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) or -33db (least sensitive).

Audio type: Select audio codec as AAC, G.711, or G.726, and the sampling bit rate .

- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (μ-Law) or pcma (A-Law) mode.
- G.726 is a speech codec standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s.

When completed with the settings on this page, click **Save** to enable the settings.

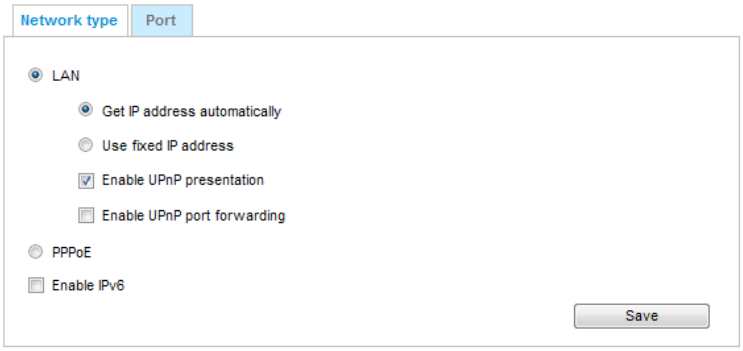
IMPORTANT:

The network camera does not come with embedded microphone. An external microphone will be necessary especially if you prefer the **Audio Detection** feature. By default, the Audio setting is muted, and you need to manually uncheck the **Mute** option.

Network > General settings

This section explains how to configure a wired network connection for the Network Camera.

Network Type

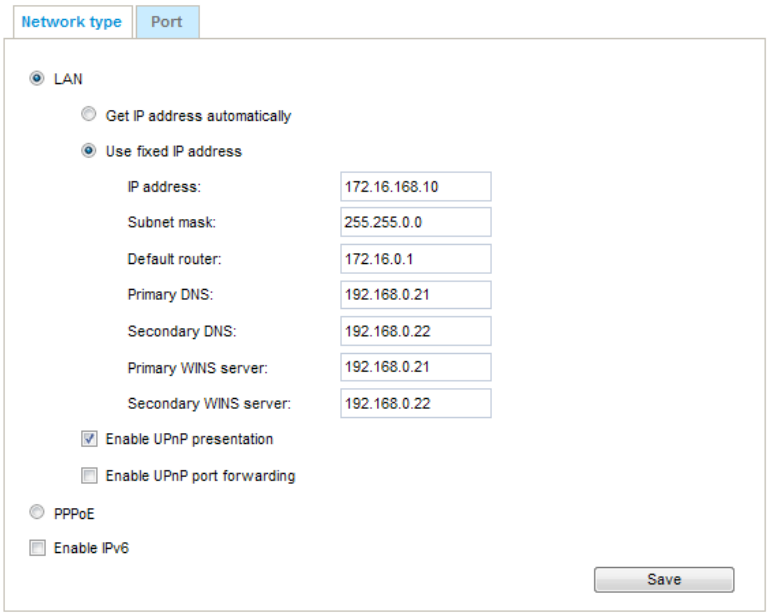


LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Please rememer to click on the **Save** button when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.



1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 17 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP or network administrator.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will disable the transmission to destinations across different subnets.

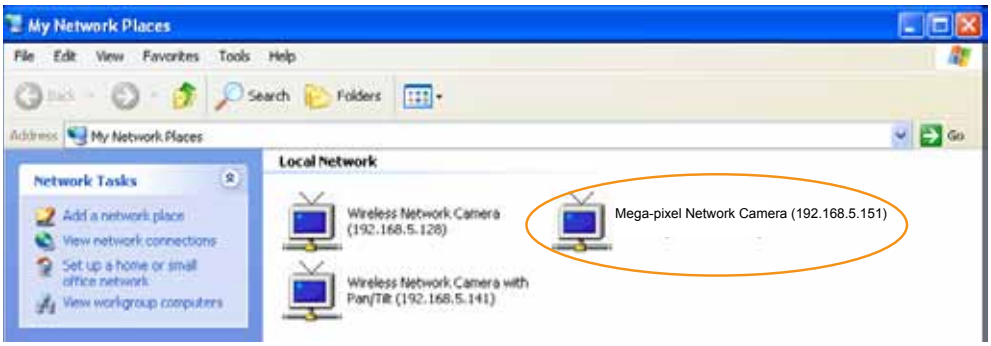
Primary DNS: The primary domain name server that translates host names into IP addresses.

Secondary DNS: Secondary domain name server that backs up the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer names and IP addresses.

Secondary WINS server: The secondary WINS server that maintains the database of computer names and IP addresses.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, the shortcuts to connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



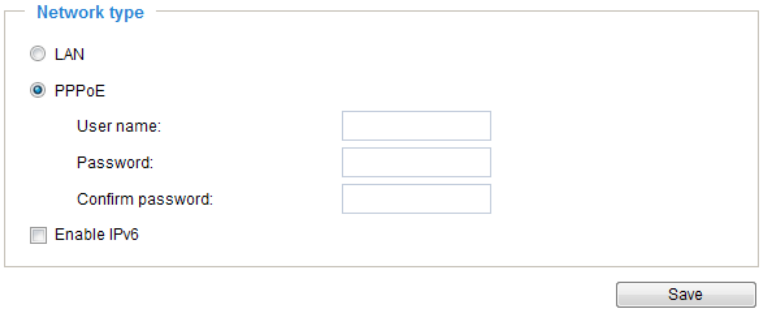
Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports automatically on the router so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Configuration > Event > Event settings > Add server (please refer to Add server on page 105) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 96). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.



5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

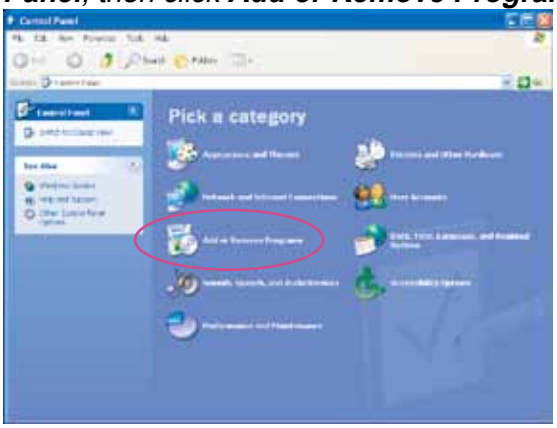
NOTE:

► *If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.*

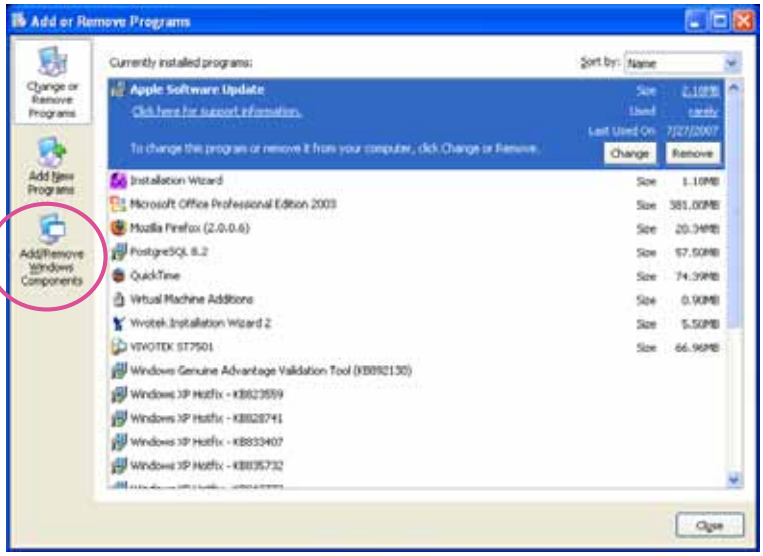
► *If UPnP™ is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

► *Steps to enable the UPnP™ user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

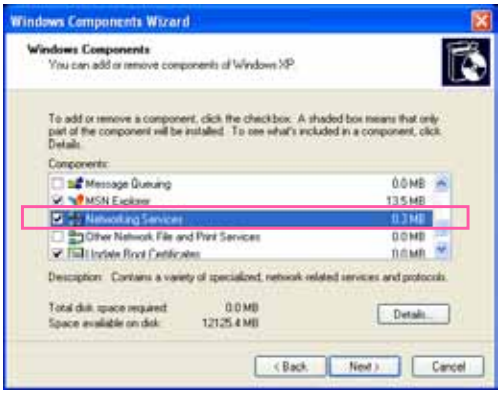
1. *Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



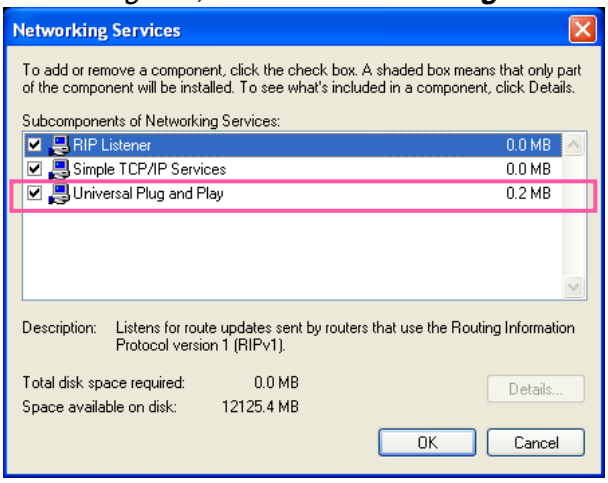
2. *In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*



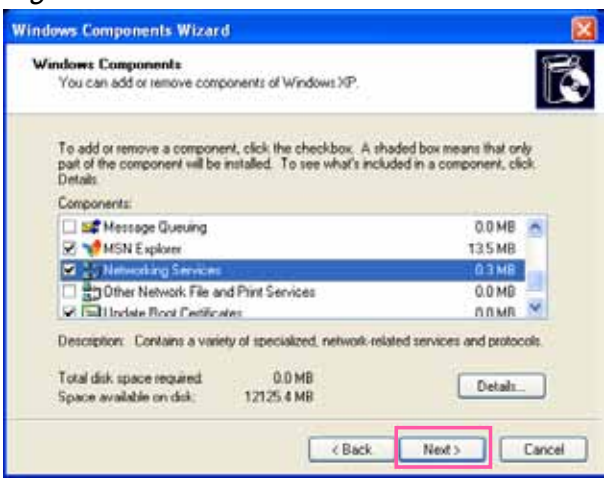
3. *In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.*



4. In the Networking Services dialog box, select ***Universal Plug and Play*** and click ***OK***.


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Listens for route updates sent by routers that use the Routing Information Protocol version 1 (RIPv1).
Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB
Details...
OK
Cancel

5. Click ***Next*** in the following window.


Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Message Queuing 0.0 MB
MSN Explorer 13.5 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 12125.4 MB
Details...
< Back
Next >
Cancel

6. Click ***Finish***. UPnP™ is enabled.

► *How does UPnP™ work?*
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

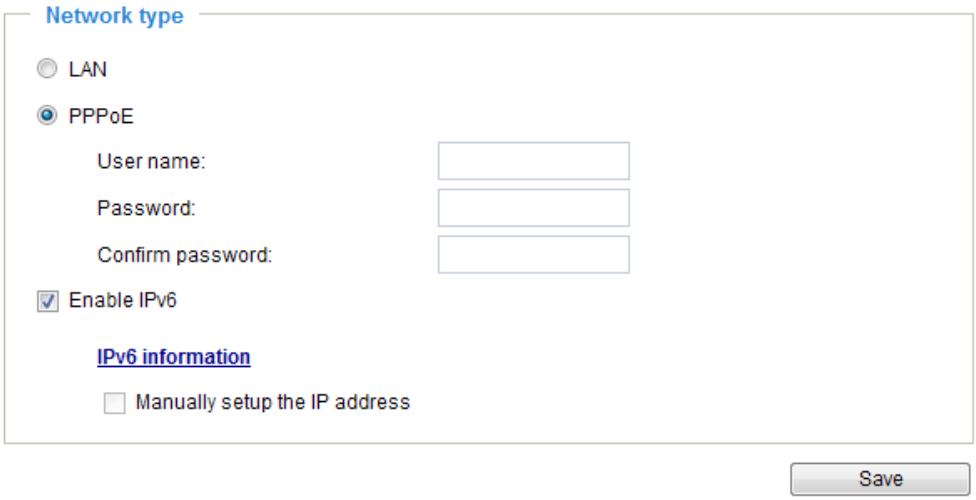
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 43 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

Enable IPv6

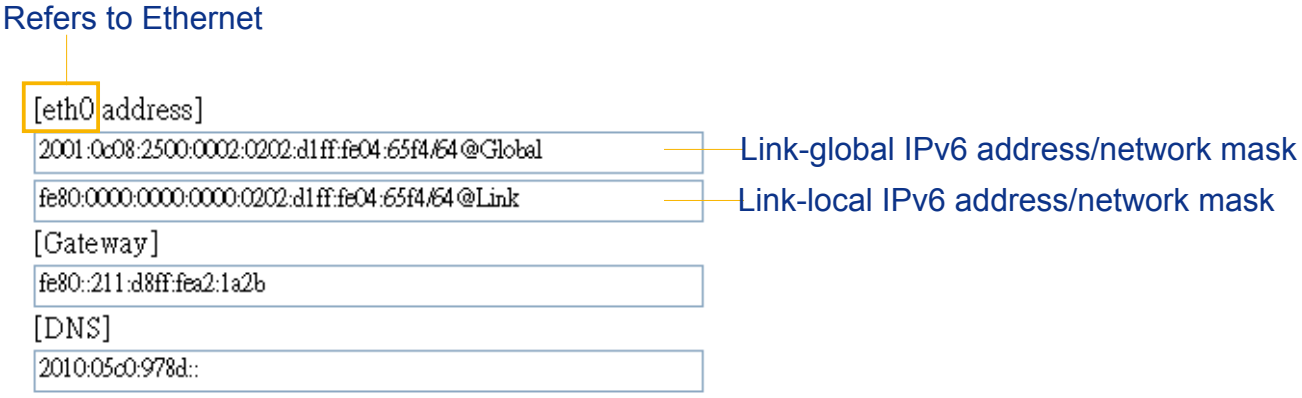
Select this option and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.



When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

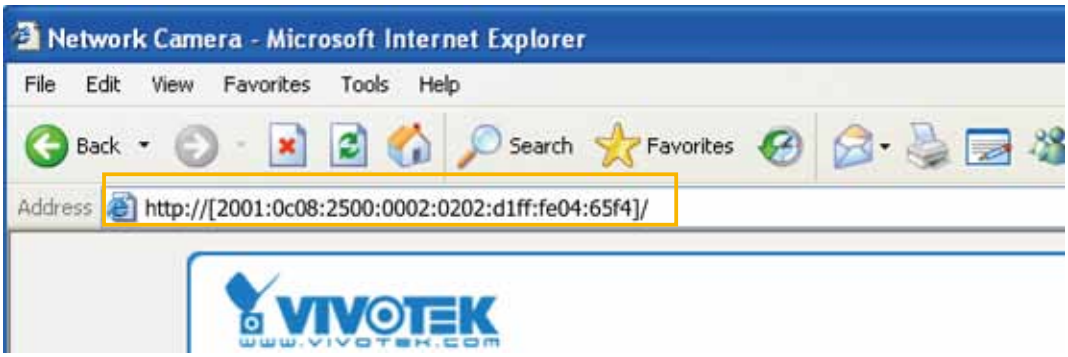
IPv6 Information: Click this button to obtain the IPv6 information as shown below.

If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:



Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

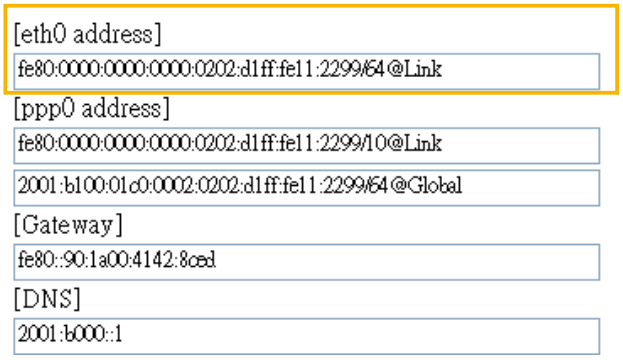
4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:



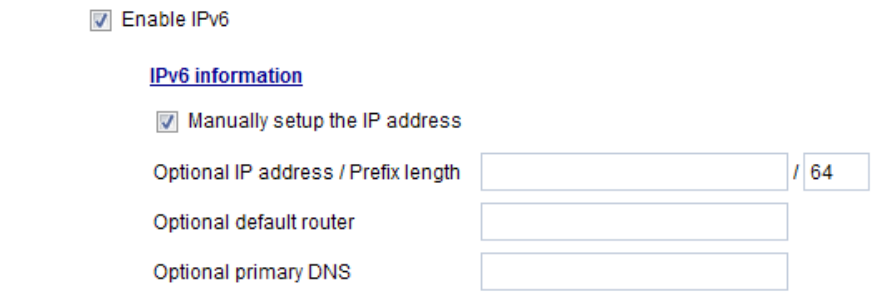
NOTE:

► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** streaming on page 68 for detailed information.)*

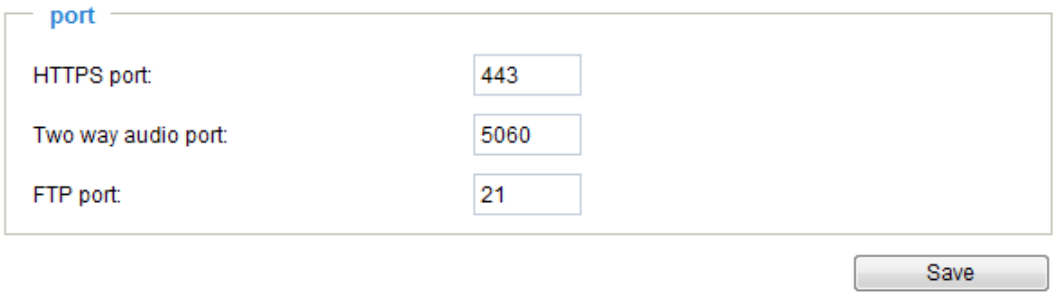
► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*



Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have a DHCPv6 server and router advertisements-enabled routers.
If you select this item, the following blanks will be displayed for you to enter the corresponding information:



Port



HTTPS port: By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two way audio port: By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" on the Media > Video > Stream settings page and the media option is set to "Media > Video > Stream settings" on the Client Settings page. Please refer to Client Settings on page 30 and Stream settings on page 57.

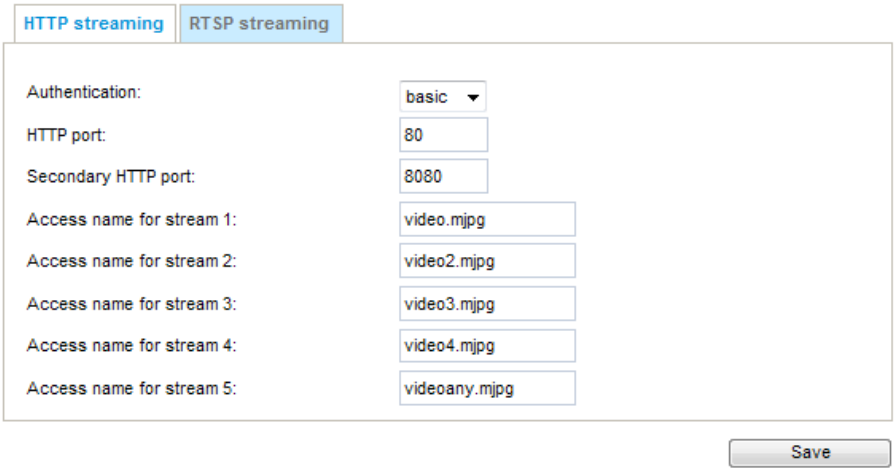
Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP port: The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

Network > Streaming protocols

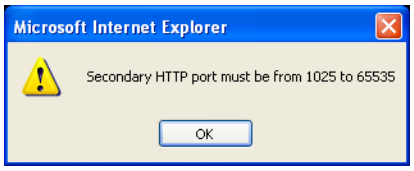
HTTP streaming

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 78 for details.



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

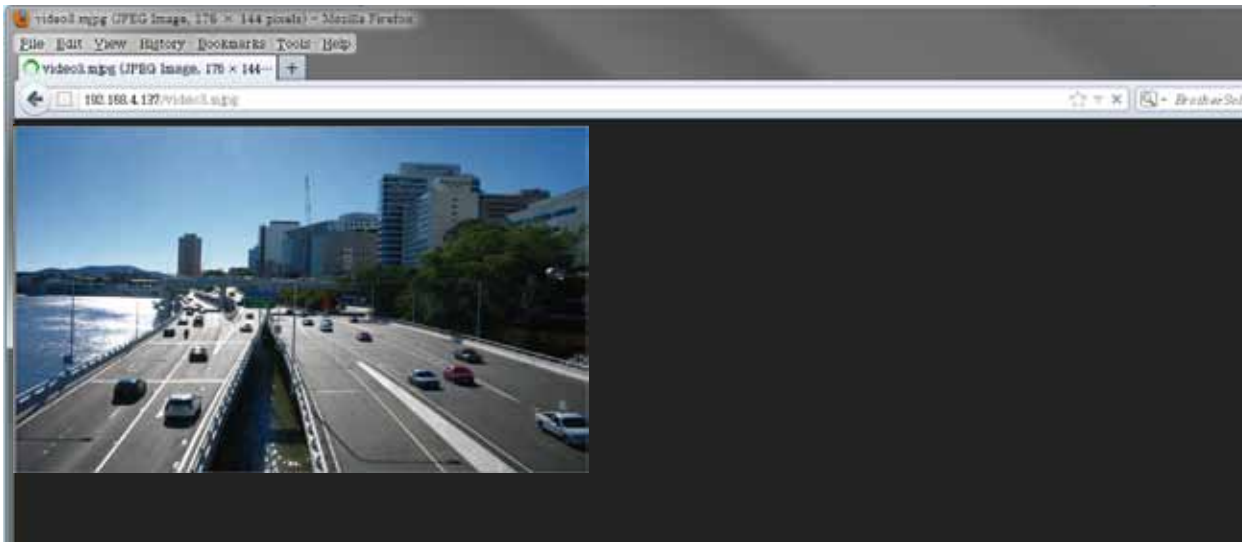
On the LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 ~ 5: This Network camera supports multiple streams simultaneously. The access name is used to identify different video streams. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 56.

When using **Mozilla Firefox** to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox.

URL command -- http://<ip address>:<http port>/<access name for stream 1, 2, 3, 4, or 5>
For example, when the Access name for stream 2 is set to video2.mjpg:

1. Launch the Mozilla Firefox browser.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.

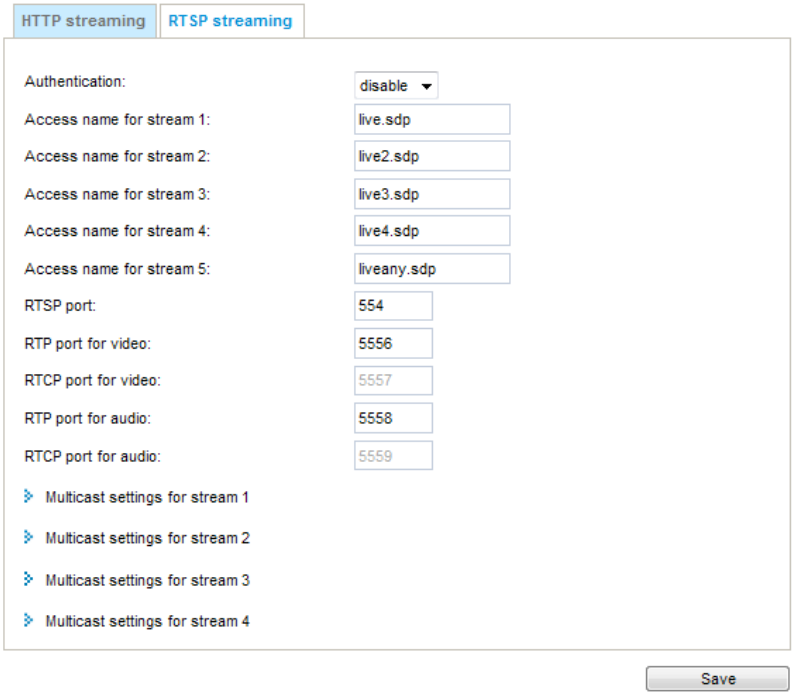


NOTE:

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1, 2, 3, 4, or 5> will not work.*

RTSP Streaming

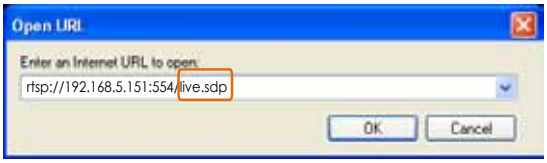
To utilize RTSP streaming authentication, make sure that you have set a password for controlling the access to video stream first. Please refer to Security > User account on page 78 for details.



Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed below:

	Quick Time player	VLC
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream 1 ~ 5: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.
If you want to use an RTSP player to access the Network Camera, you have to set the video mode to H.264 / MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream 1 to 5>
For example, when the access name for stream 1 is set to live.sdp:
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.



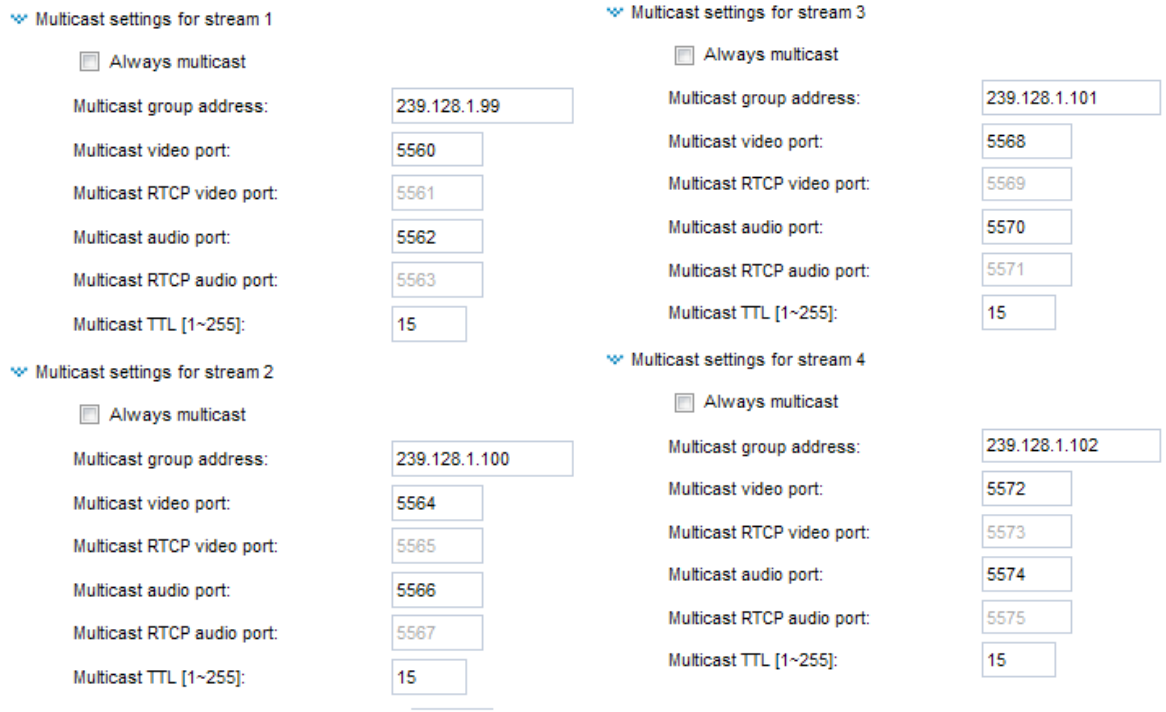
RTSP port /RTP port for video, audio/ RTCP port for video, audio

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:

Multicast settings for stream 1, 2, 3, and 4: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for video streams.


Multicast settings for stream 1
Always multicast
Multicast group address: 239.128.1.99
Multicast video port: 5560
Multicast RTCP video port: 5561
Multicast audio port: 5562
Multicast RTCP audio port: 5563
Multicast TTL [1~255]: 15
Multicast settings for stream 2
Always multicast
Multicast group address: 239.128.1.100
Multicast video port: 5564
Multicast RTCP video port: 5565
Multicast audio port: 5566
Multicast RTCP audio port: 5567
Multicast TTL [1~255]: 15
Multicast settings for stream 3
Always multicast
Multicast group address: 239.128.1.101
Multicast video port: 5568
Multicast RTCP video port: 5569
Multicast audio port: 5570
Multicast RTCP audio port: 5571
Multicast TTL [1~255]: 15
Multicast settings for stream 4
Always multicast
Multicast group address: 239.128.1.102
Multicast video port: 5572
Multicast RTCP video port: 5573
Multicast audio port: 5574
Multicast RTCP audio port: 5575
Multicast TTL [1~255]: 15

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:

Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

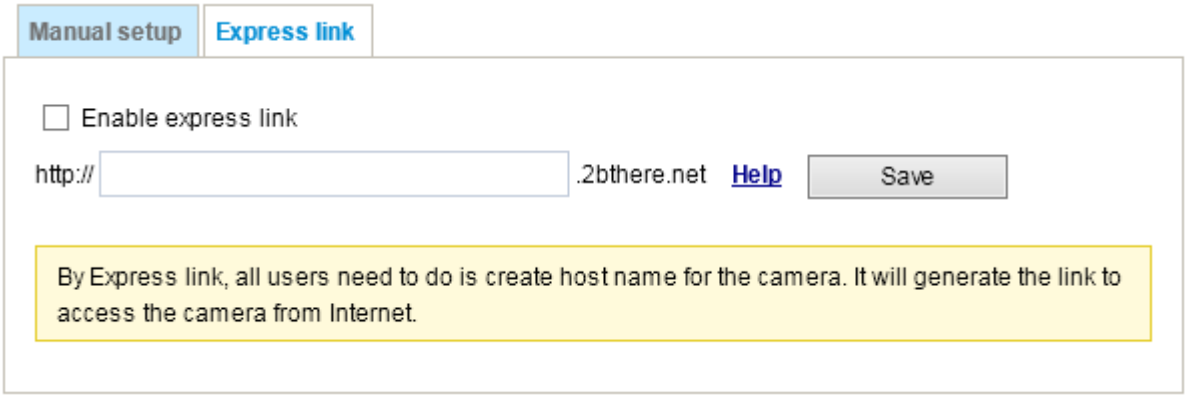
Initial TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

Network > DDNS

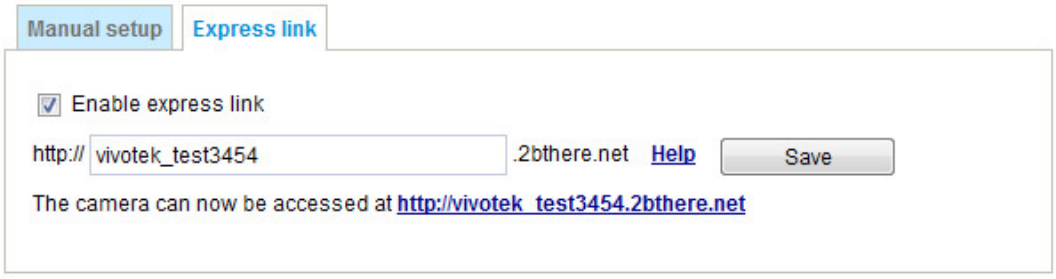
This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

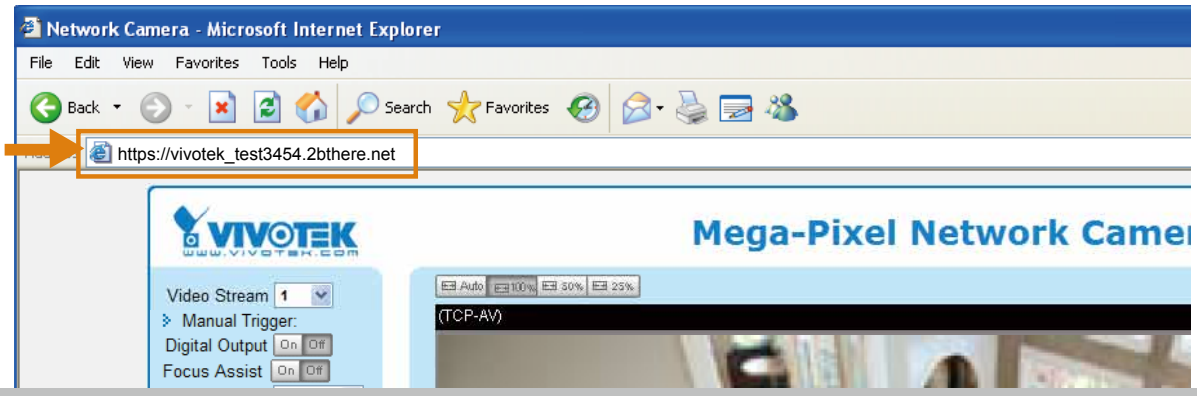
Express link

Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will examine if the host name is valid and automatically open a port on your router. If using DDNS, the user has to manually configure UPnP port forwarding. Express Link is more convenient and easier to set up.


Manual setup
Express link
Enable express link
http://
.2bthere.net
Help
Save
By Express link, all users need to do is create host name for the camera. It will generate the link to access the camera from Internet.

Please follow the steps below to enable Express Link:
1. Make sure that your router supports UPnP port forwarding and it is activated.
2. Check **Enable express link**.
3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will display a message as shown below.





Manual setup

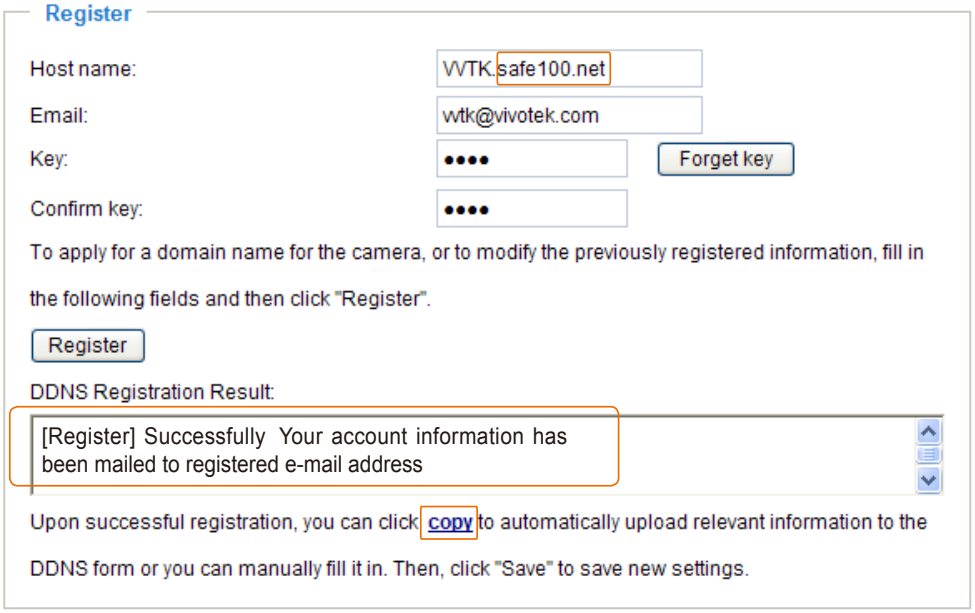
DDNS: Dynamic domain name service

Enable DDNS: Select this option to enable the DDNS setting.

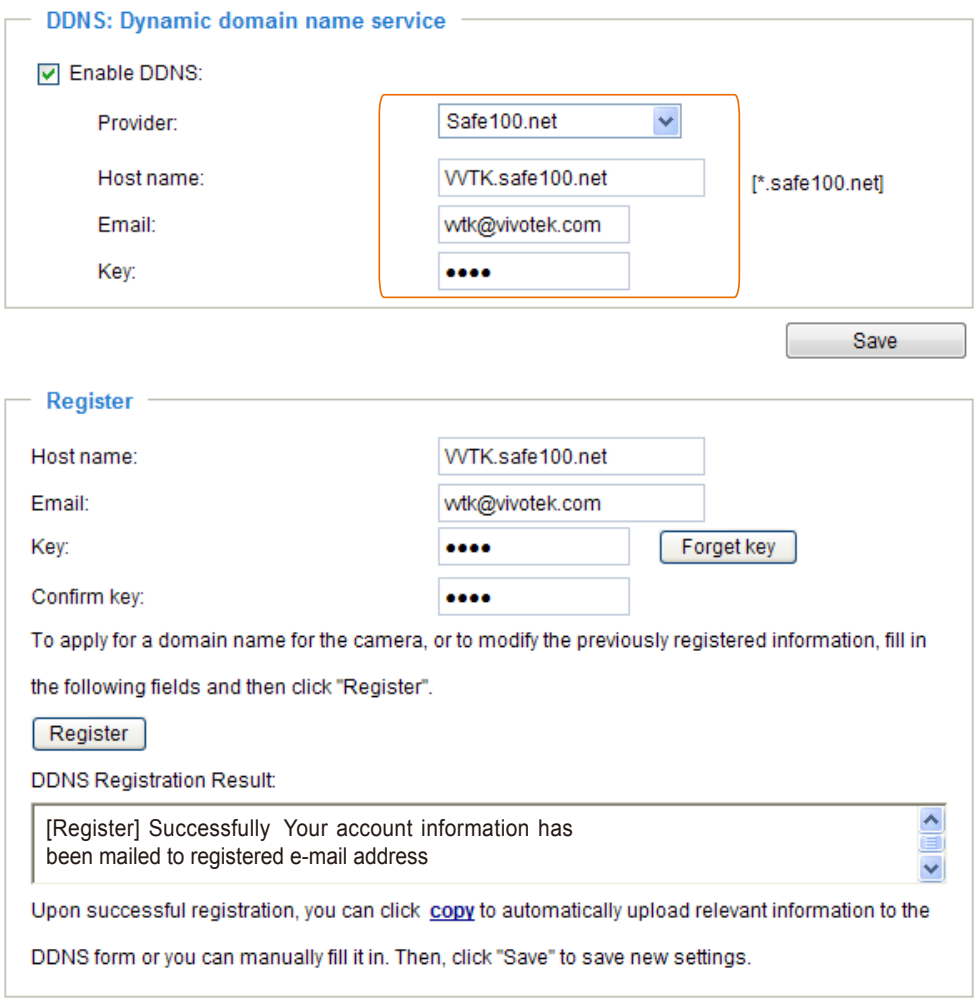
Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.


Register
Host name:
VVTK.safe100.net
Email:
vtk@vivotek.com
Key:
Forget key
Confirm key:
To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".
Register
DDNS Registration Result:
[Register] Successfully Your account information has been mailed to registered e-mail address
Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.


DDNS: Dynamic domain name service
Enable DDNS:
Provider:
Safe100.net
Host name:
VVTK.safe100.net
[*.safe100.net]
Email:
vtk@vivotek.com
Key:
Save
Register
Host name:
VVTK.safe100.net
Email:
vtk@vivotek.com
Key:
Forget key
Confirm key:
To apply for a domain name for the camera, or to modify the previously registered information, fill in the following fields and then click "Register".
Register
DDNS Registration Result:
[Register] Successfully Your account information has been mailed to registered e-mail address
Upon successful registration, you can click copy to automatically upload relevant information to the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.

4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Server name, Email, Key, and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a success message in the DDNS Registration Result column. Enter **ns1.safe100.net** as the Server name.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/

Network > QoS (Quality of Service)

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:

- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:

- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates the frame priority level from 0 (lowest) to 7 (highest). The priority is set up via a web console with the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).

If you assign Video the highest level, the switch will handle video packets first.

NOTE:

► *A VLAN Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.*

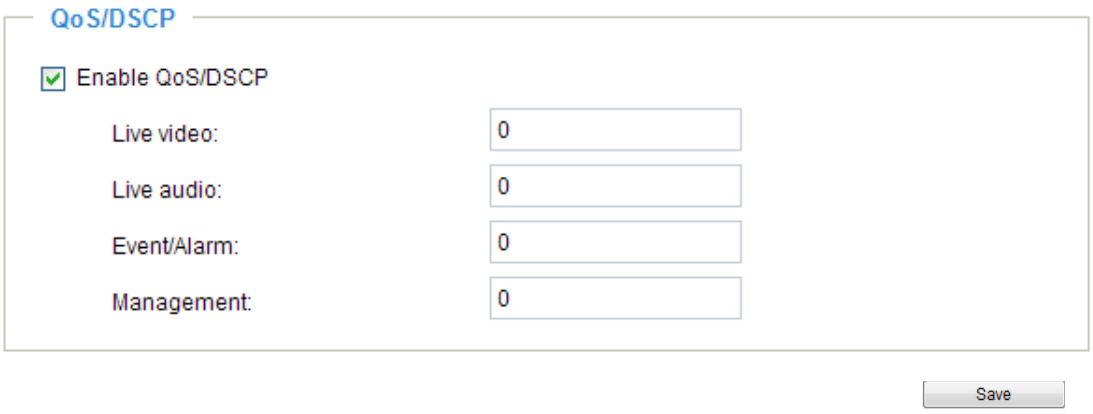
► *Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).



Network > SNMP (Simple Network Management Protocol)

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c
Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.

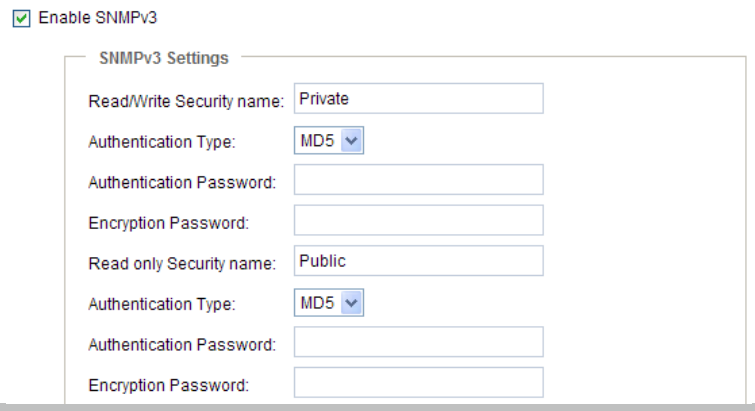
Enable SNMPv3
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authentication (at least 8 characters).

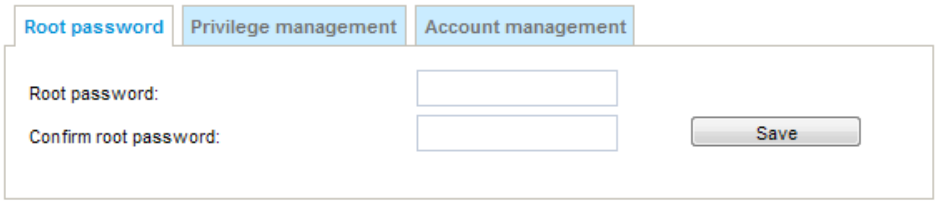
■ Encryption password: Enter a password for encryption (at least 8 characters).



Security > User Account

This section explains how to enable password protection and create multiple accounts.

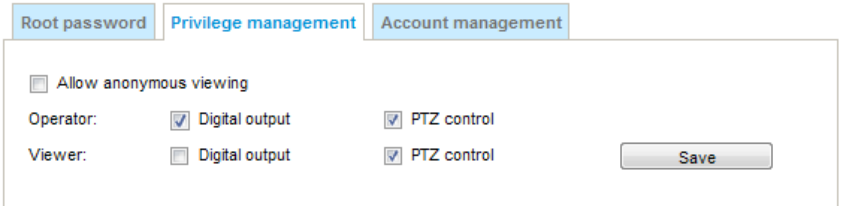
Root Password



The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the “root” account first.

1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will prompt for authentication; type the correct user’s name and password in their respective fields to access the Network Camera.

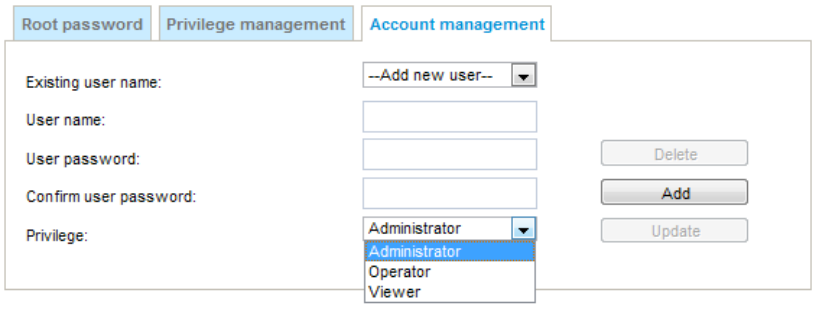
Privilege management



Digital Output & PTZ control: You can modify the manage privileges of operators or viewers. Select or deselect the checkboxes, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 35).

Allow anonymous viewing: If this checkbox is selected, any client can access the live stream without entering a User ID and Password.

Account management



Administrators can add up to 20 user accounts.

1. Input the new user’s name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Although operators cannot access the Configuration page, they can use the URL Commands to get and set the camera parameters. For more information, please refer to URL Commands of the Network Camera at the Appendix of this manual. Viewers access only the main page for live viewing.

Here you also can change a user’s access rights or delete user accounts.

1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

Security > HTTPS (Hypertext Transfer Protocol over SSL)

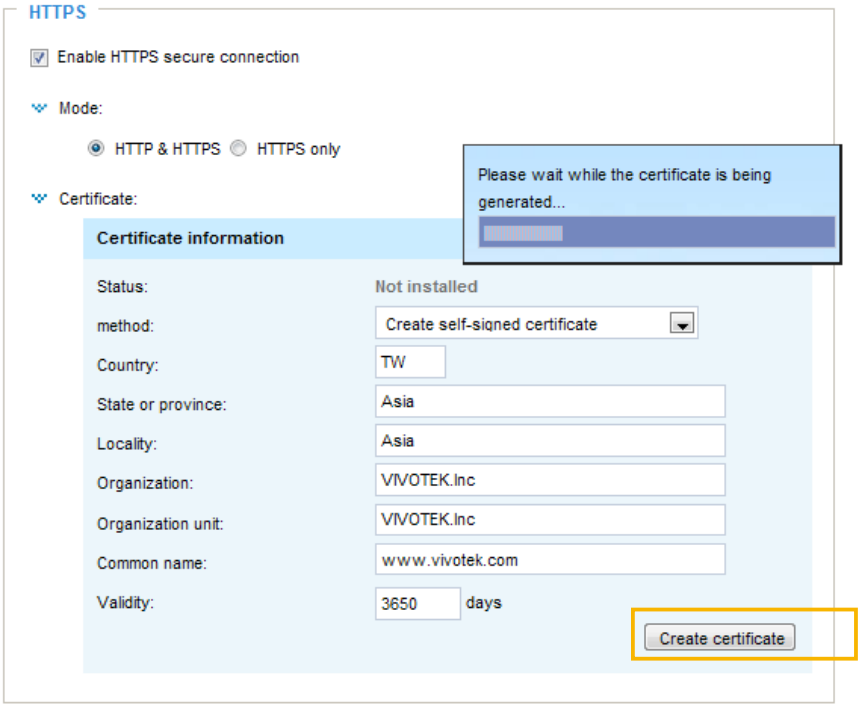
This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

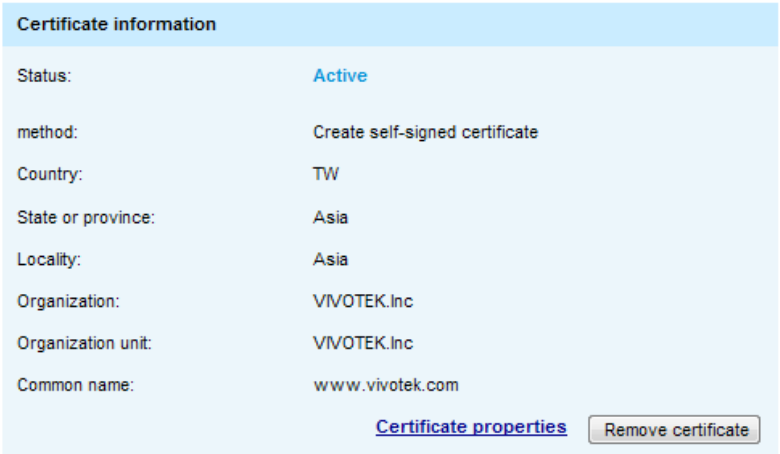
Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate

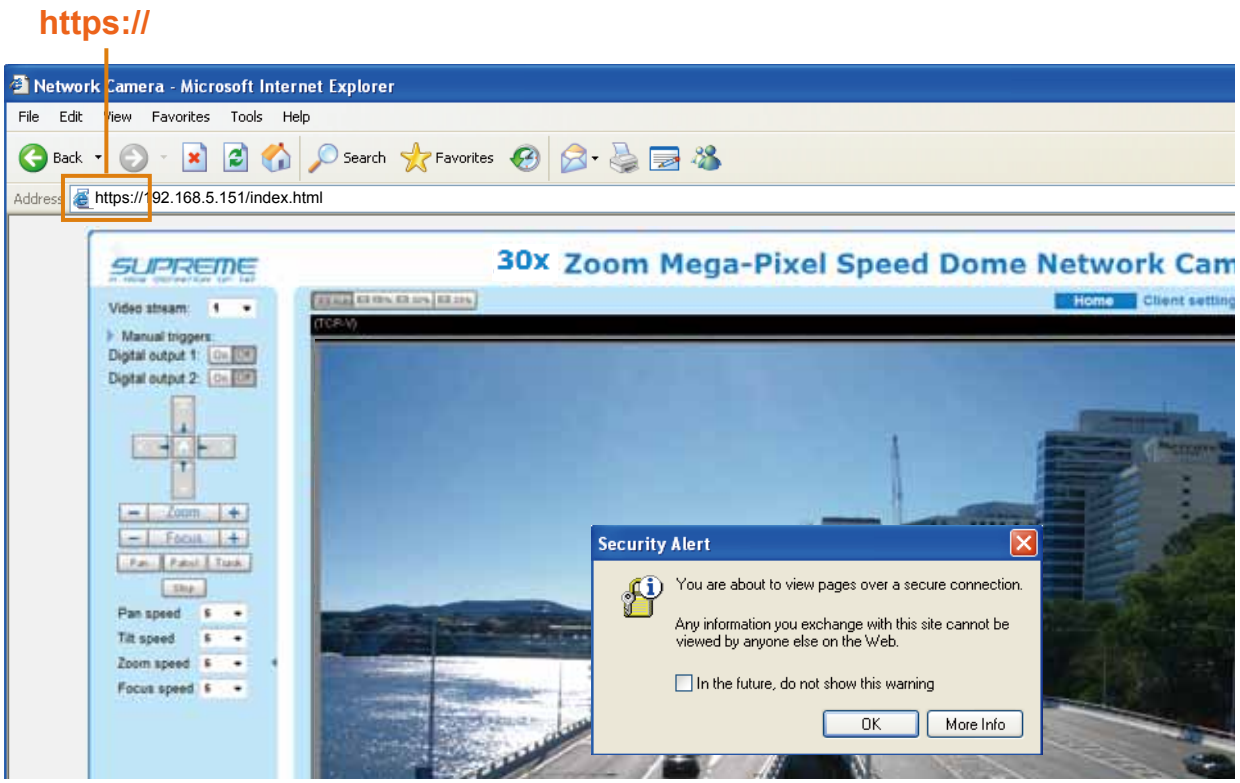
1. Select this option from a pull-down menu.
2. In the first column, select **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Create certificate** to generate a certificate.



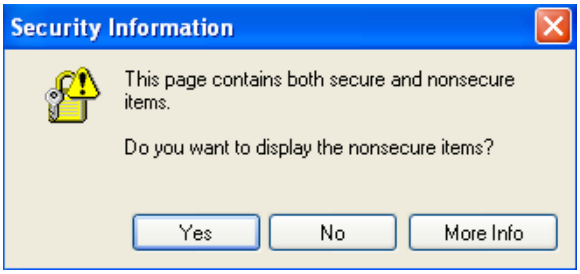
4. The Certificate Information will automatically be displayed as shown below. You can click **Certificate properties** to view detailed information about the certificate.



5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
6. If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

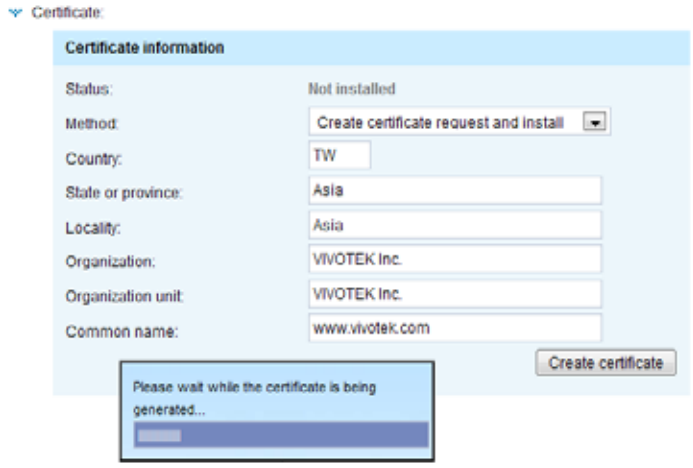


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

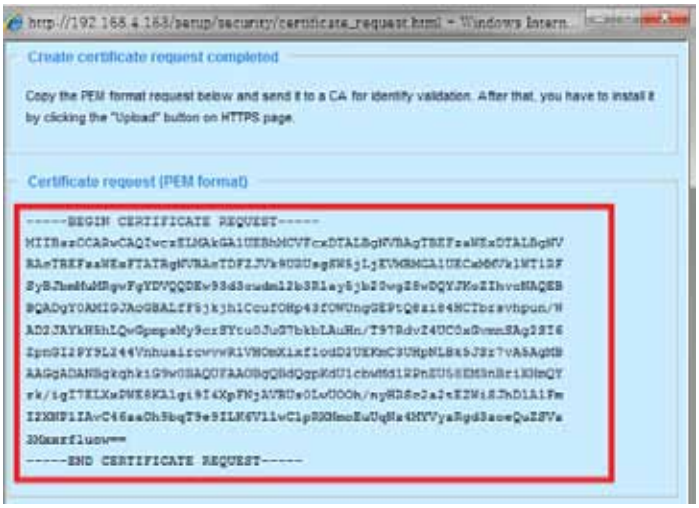


Create certificate request and install

1. Select the option from the **Method** pull-down menu.
2. Click **Create certificate** to proceed.
3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate request.



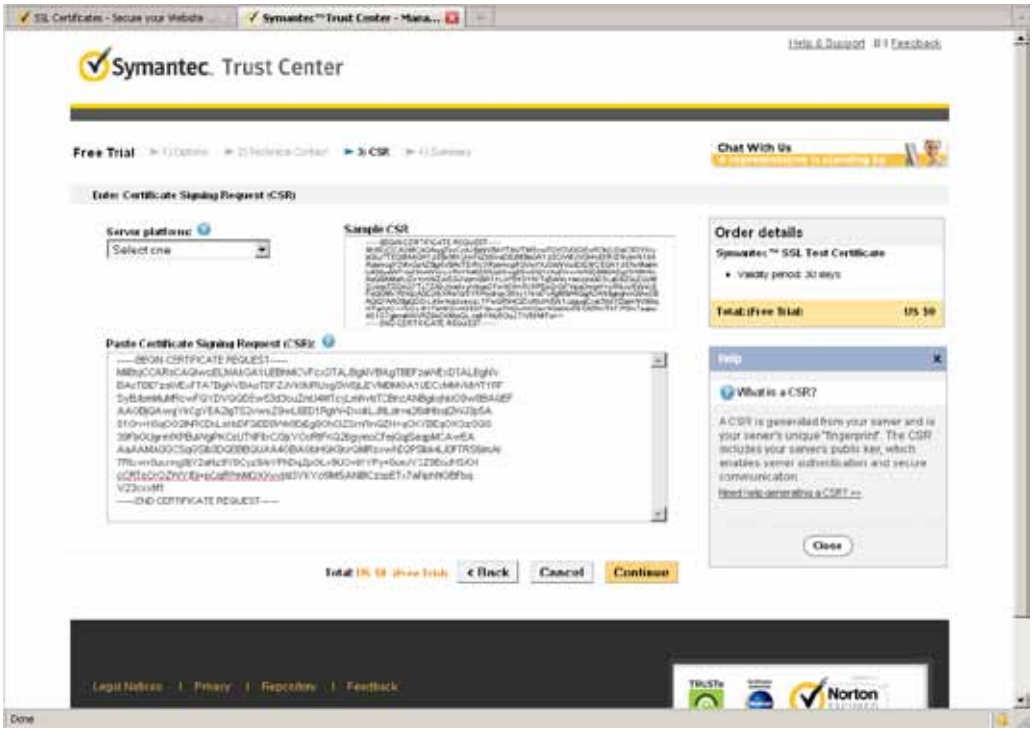
4. The Certificate request window will prompt.


Create certificate request completed
Copy the PEM format request below and send it to a CA for identity validation. After that, you have to install it by clicking the "Upload" button on HTTPS page.
Certificate request (PEM format)
-----BEGIN CERTIFICATE REQUEST-----
-----END CERTIFICATE REQUEST-----

If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.

HTTPS - Microsoft Internet Explorer
Pop-up blocked. To see this pop-up or additional options click here...
VIVOTEK
Home
Configuration
Language
Security > HTTPS
System
Security
User account
HTTPS
Access list
IEEE 802.1x
Network
Information Bar
Did you notice the Information Bar?
The Information Bar alerts you when Internet Explorer blocks a pop-up window or file download that might not be safe. If a Web page does not display properly, look for the Information Bar (near the top of your browser).
Do not show this message again.
Learn about the Information Bar...
OK

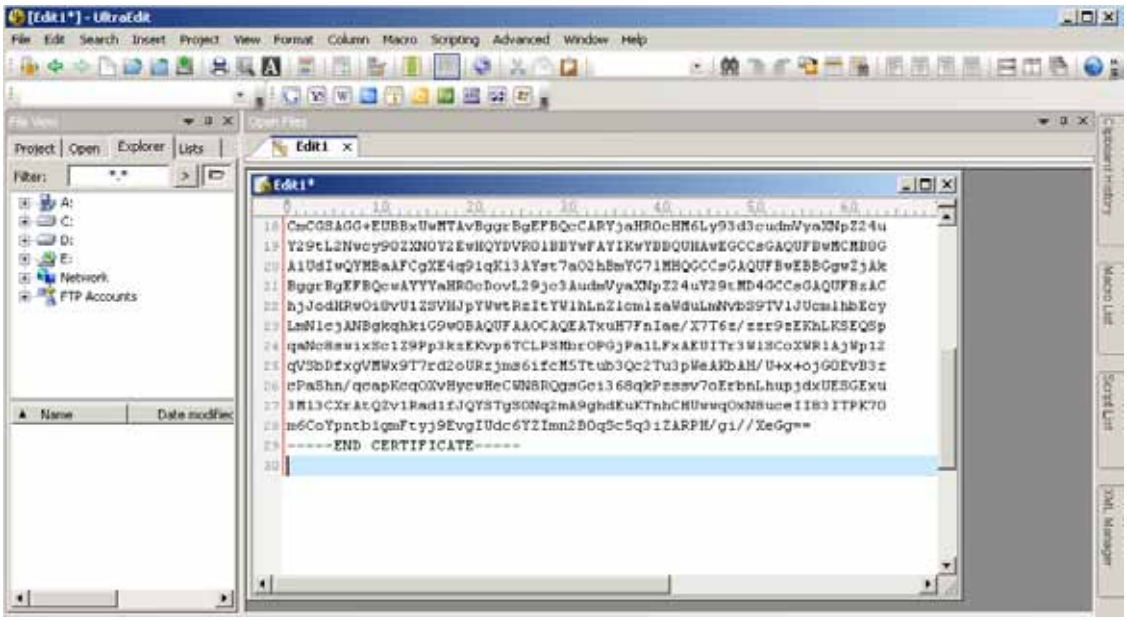
5. Look for a trusted certificate authority, such as Symantec's VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the CA's signing request window. Proceed with the rest of the process as CA's instructions on their webpage.



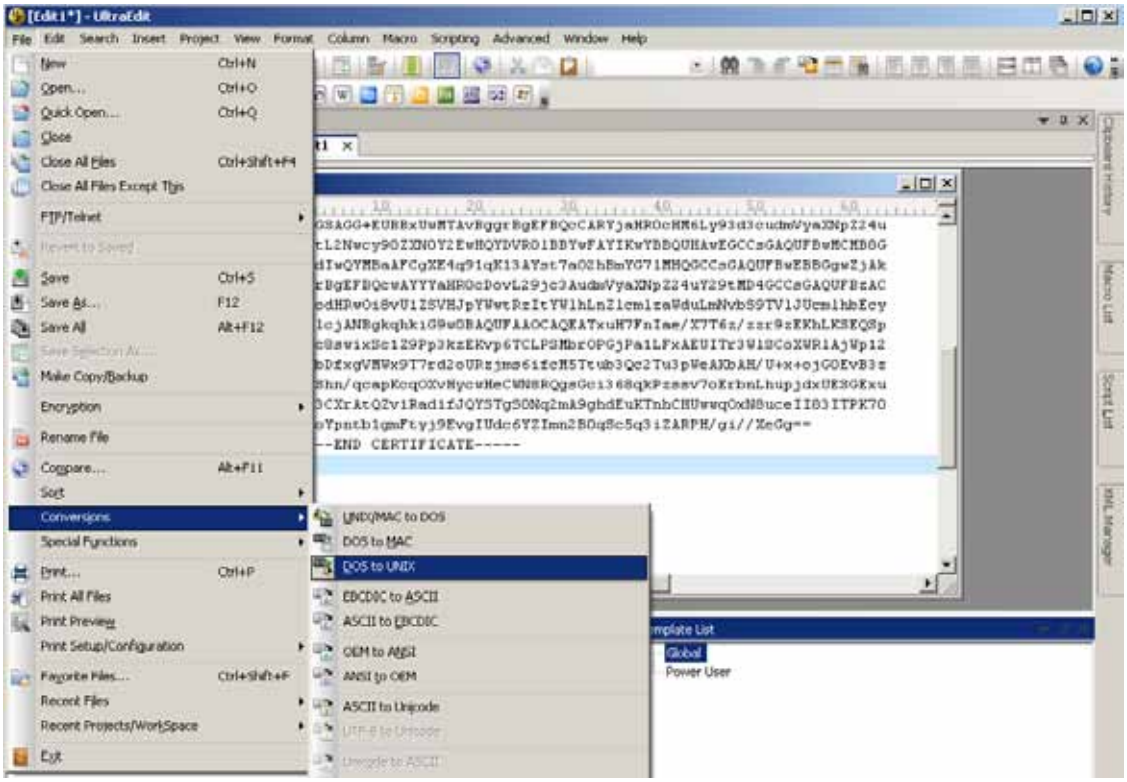
6. Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions' UltraEdit.

immediately, please dial 866.893.6565 or 650.426.5112 option 3 or send an email to internet-sales@verisign.com
Thank you for your interest in Symantec!
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

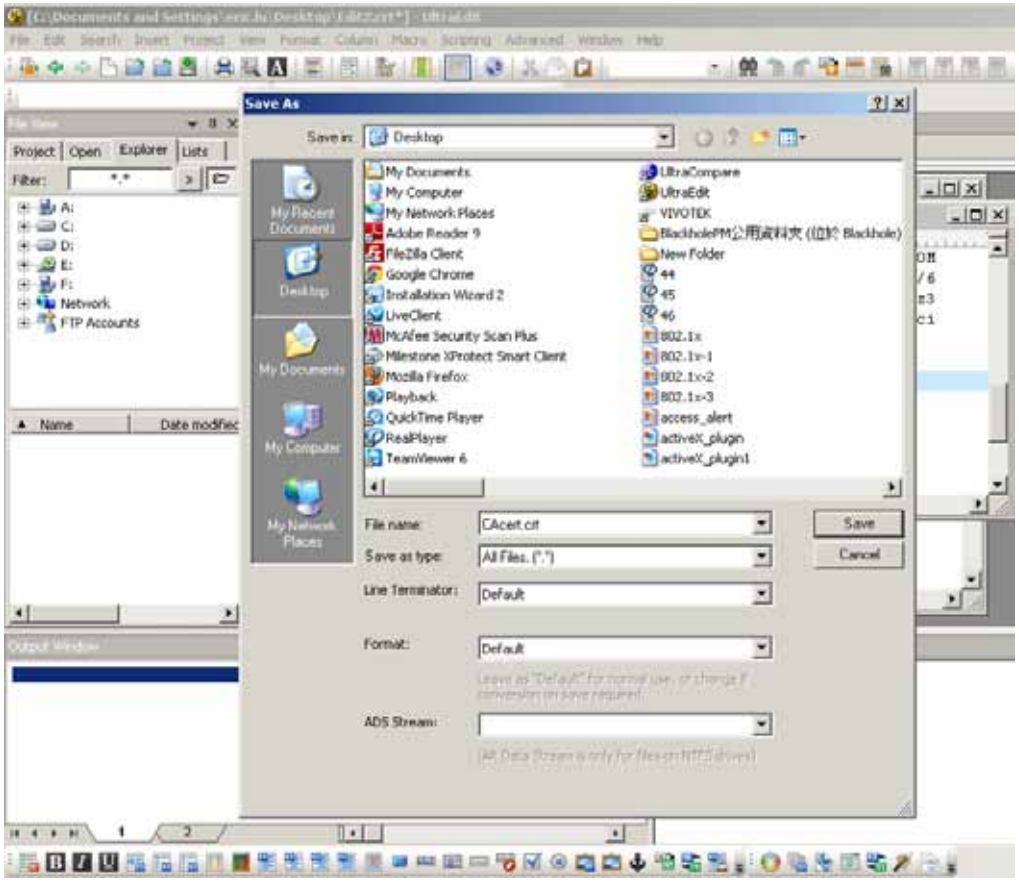
7. Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.



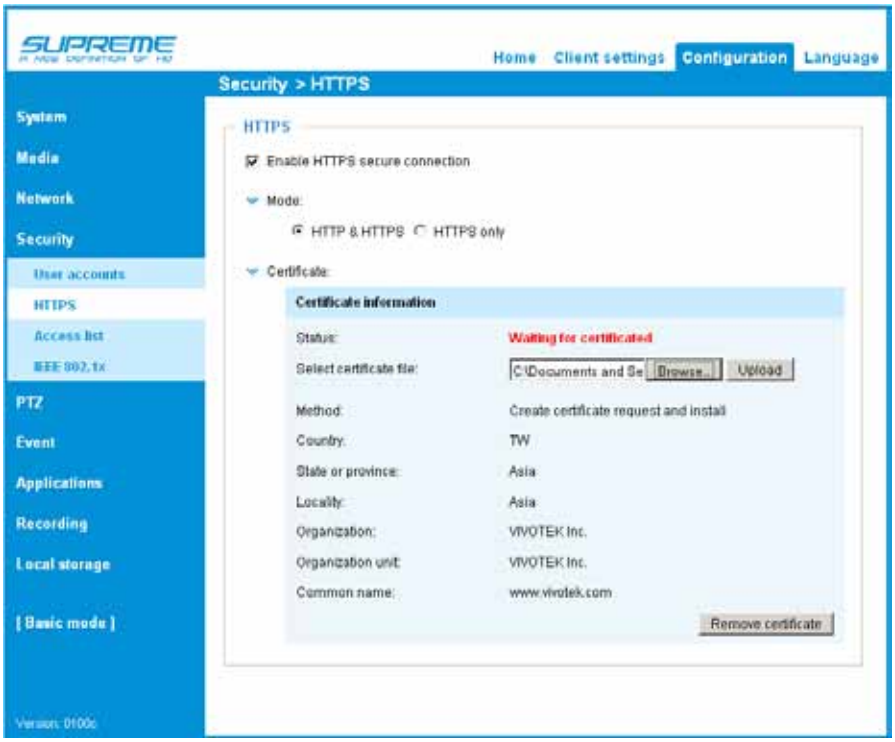
8. Convert file format from DOS to UNIX. Open **File** menu > **Conversions** > **DOS to Unix**.



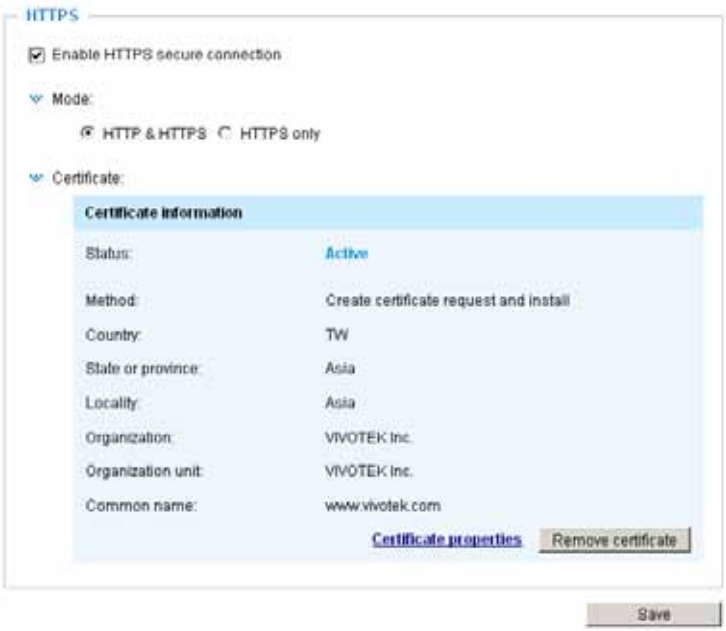
9. Save the edit using the ".crt" extension, using a file name like "CAcert.crt."



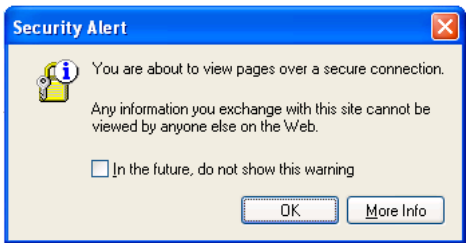
10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.

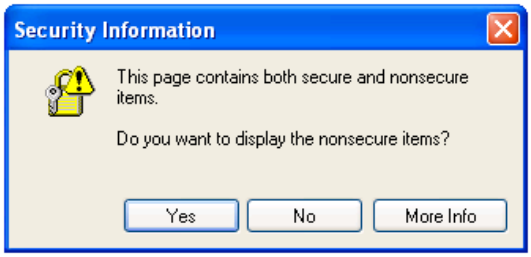


11. When the certifice file is successfully loaded, its status will be stated as **Active**. Note that a certificate must have been created and installed before you can click on the "**Save**" button for the configuration to take effect.



12. To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.


Security Alert
You are about to view pages over a secure connection.
Any information you exchange with this site cannot be viewed by anyone else on the Web.
In the future, do not show this warning
OK
More Info

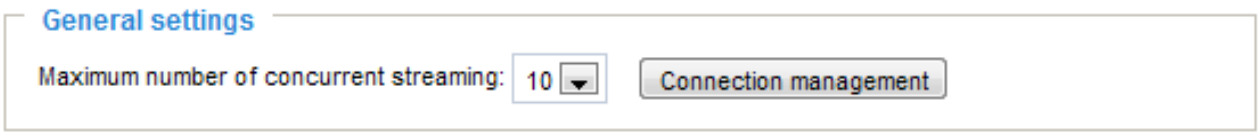


Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Security > Access List

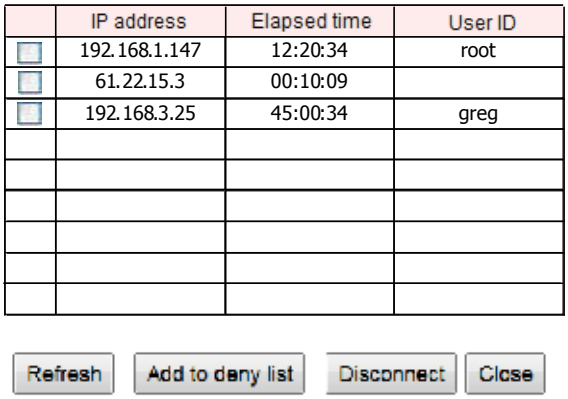
This section explains how to control access permission by verifying the client PC's IP address.

General Settings



Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including all streams). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explorer or Quick Time Player).

Connection management: Click this button to display the connection status window showing a list of the current connections. For example:



■ IP address: Current connections to the Network Camera.

■ Elapsed time: How long the client has been at the live view webpage (note that only clients currently at the live view window will be listed here).

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to make a connection without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security > User account on page 78.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 69.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to page 78.

■ Refresh: Click this button to refresh all current connections.

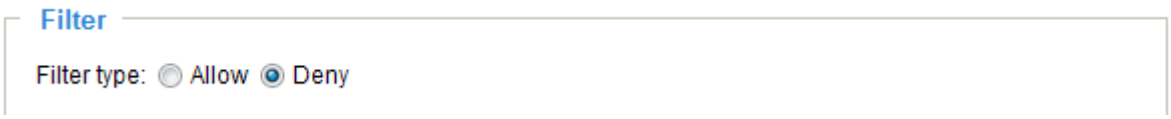
■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny their access. Please note that those checked connections will only be disconnected temporarily and they will automatically retry a connection (IE Explorer or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and they will automatically retry a connection (IE Explore or Quick Time Player).

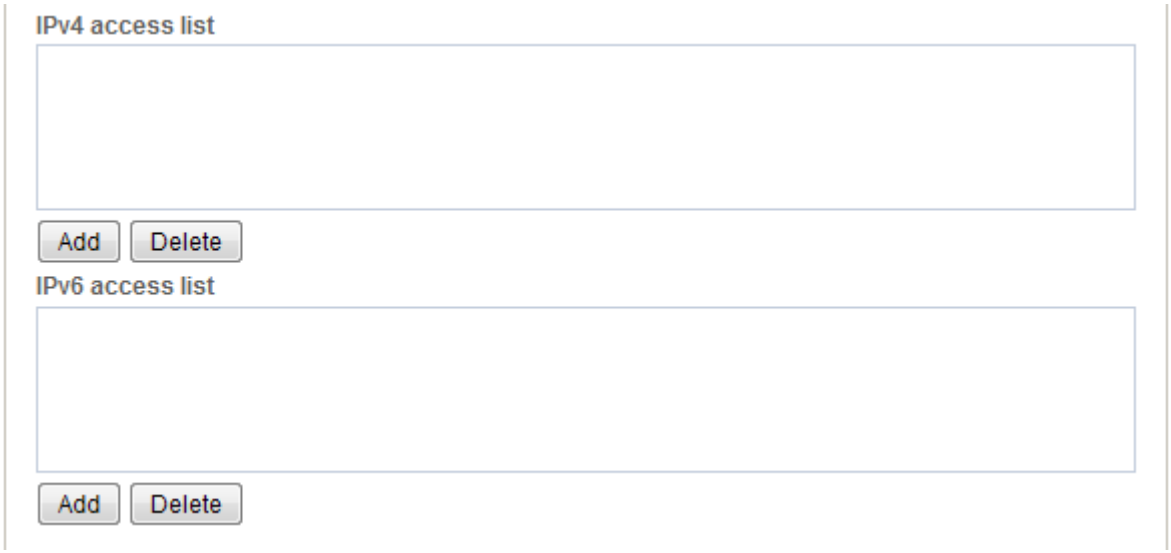
Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter

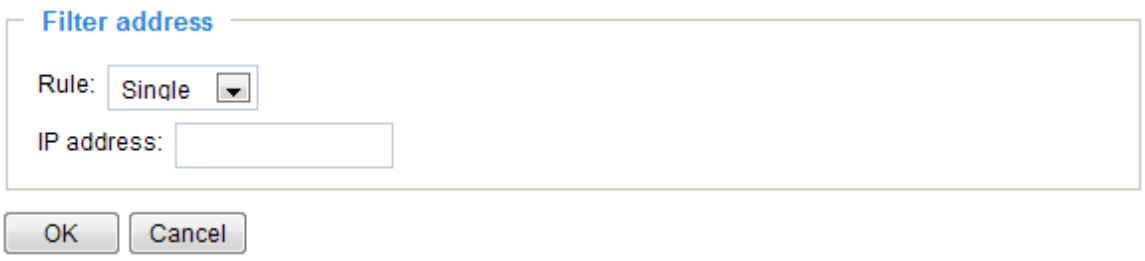
Filter type: Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and exclude the access from those that are not on the list. If you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, while those that are not on the list can.



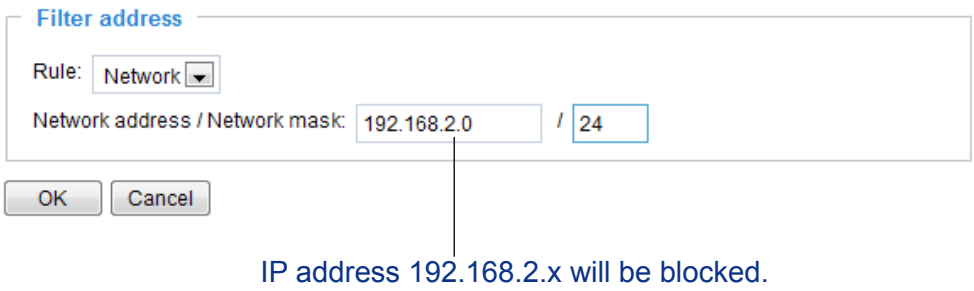
Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > Enable IPv6 on page 64 for detailed information.



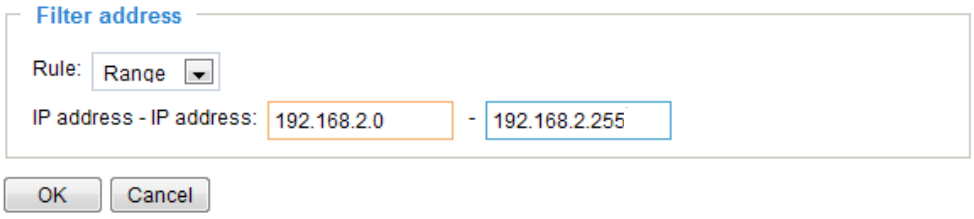
There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:



Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List in the CIDR format, e.g. 192.168.xx.xx/24.
For example:

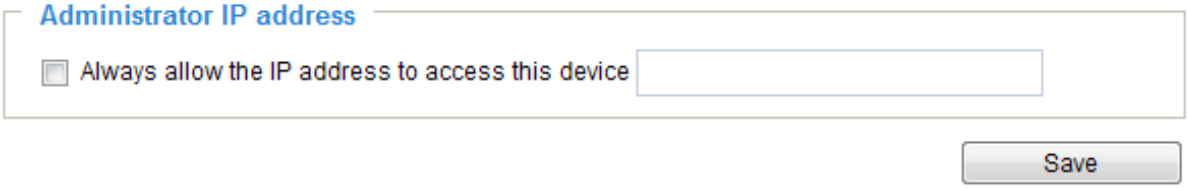


Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.
Note: This rule is only applicable to IPv4 addresses.
For example:



Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.



Security > IEEE 802.1x

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and have their 802.1x settings enabled.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:

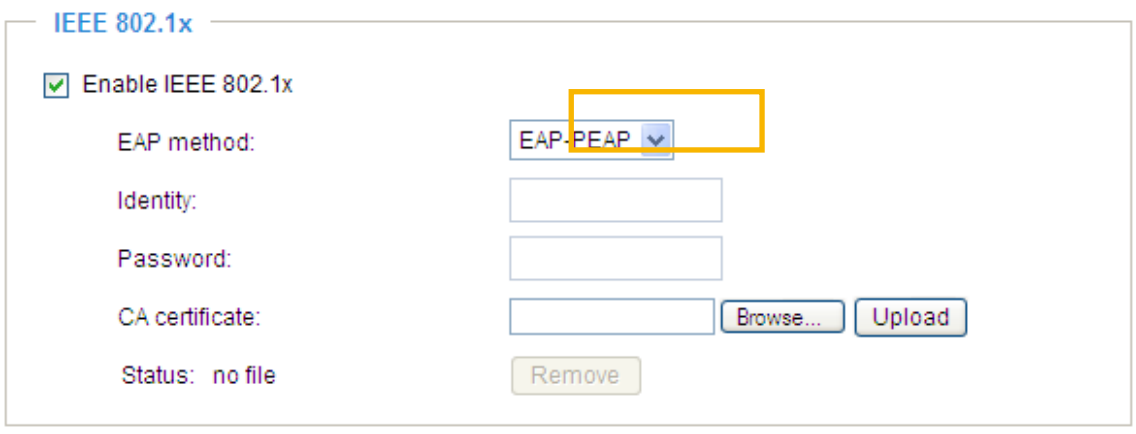
Supplicant (Network Camera) | Authenticator (Network Switch) | Authentication Server (RADIUS Server)

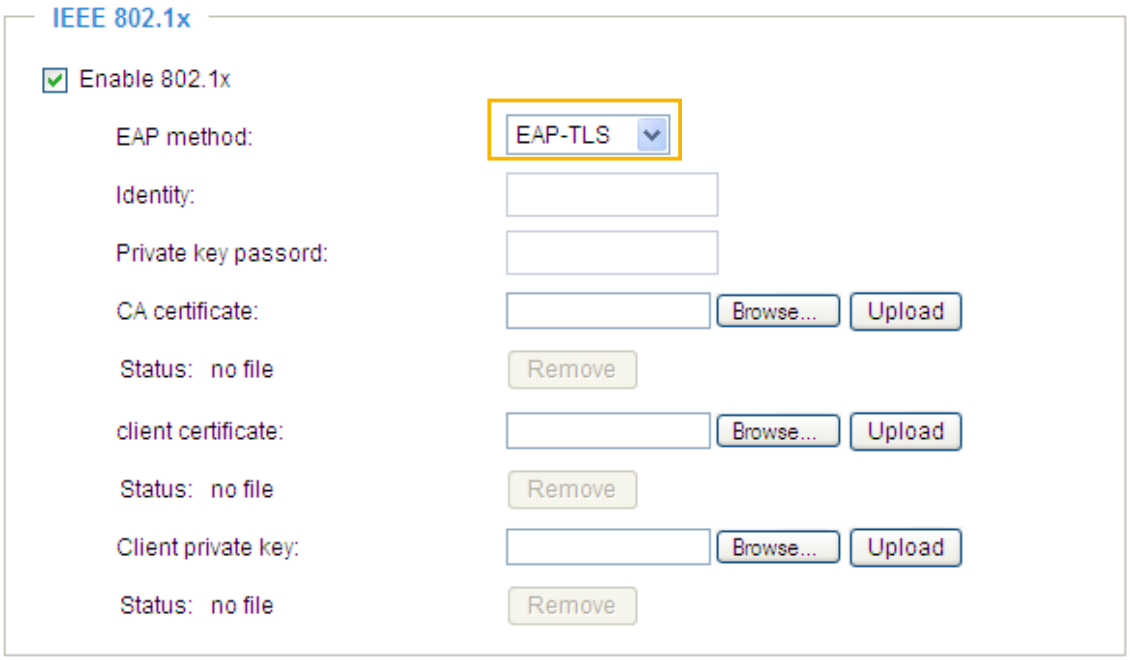
1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A “go between” which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user’s access request.

■ VIVOTEK Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:

1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (i.e., network administrator of your company) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).



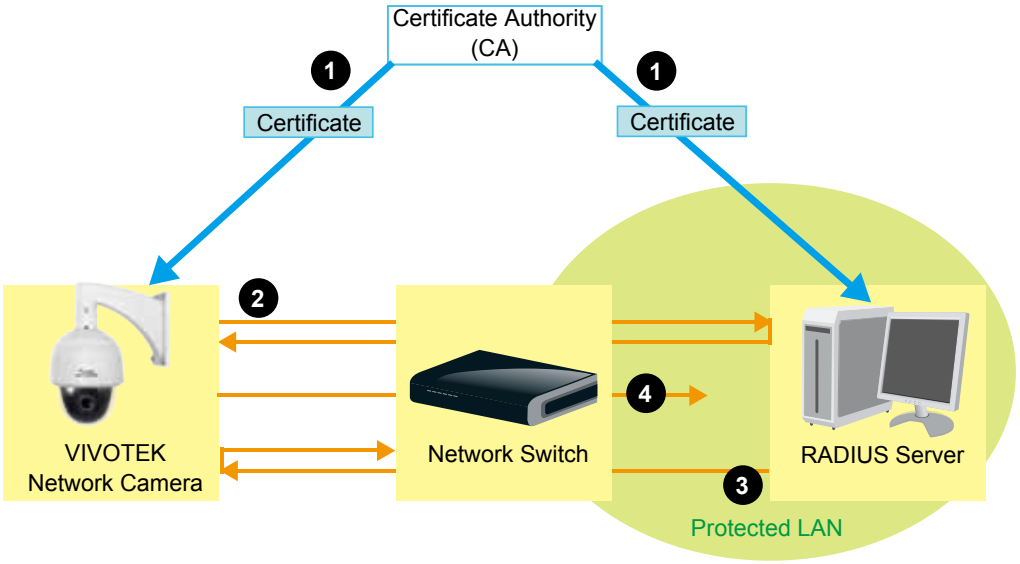


3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

NOTE:

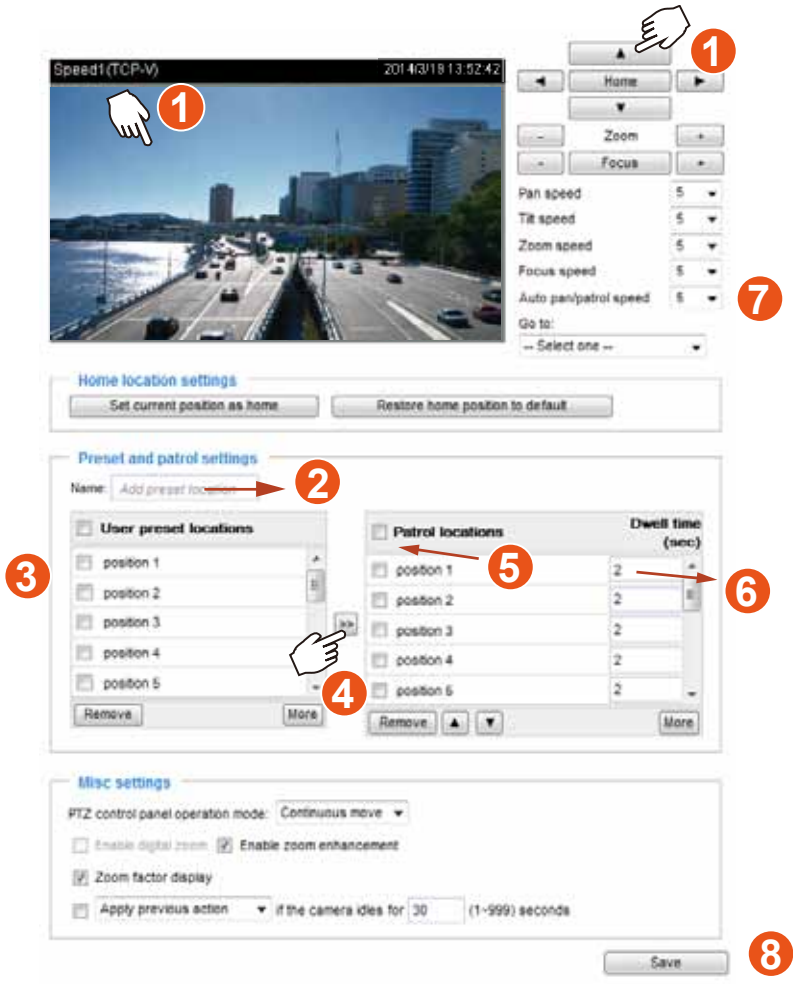
► *Below is the authentication process for 802.1x:*

1. *The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).*
2. *A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.*
3. *The switch also forwards the RADIUS Server's certificate to the Network Camera.*
4. *Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.*



PTZ > PTZ settings

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation.
The camera comes with built-in PTZ mechanisms.



NOTE:

The navigation buttons here also support the continuous move. You can click and hold down the button to move across the screen until you release the button.

Preset positions and patrol settings

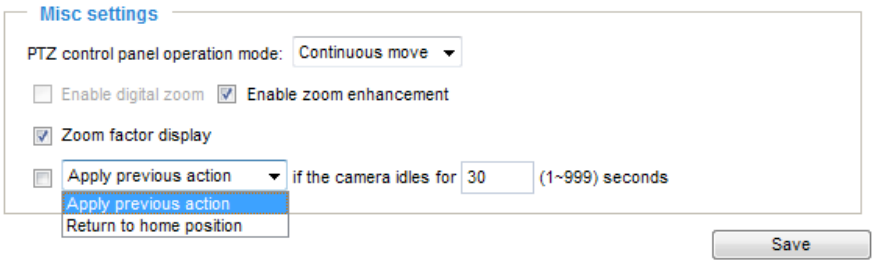
In the PTZ settings page, you can select preset positions for the camera to patrol. A total of 256 preset positions can be configured. 40 of them can be used for patrolling.

Please follow the steps below to configure preset positions and arrange them in a pan/tilt/zoom tour:

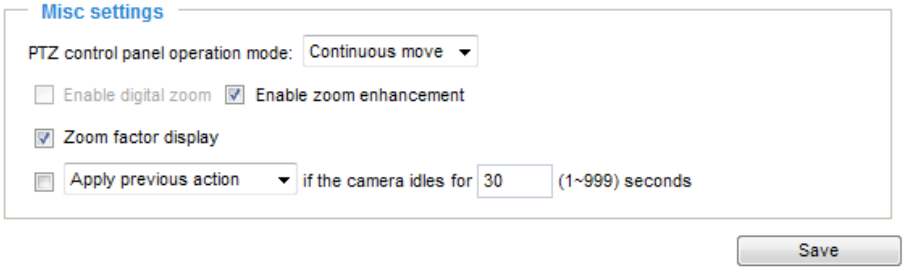
1. Adjust the shooting area to the desired position using the keypad on the upper right side of the window. The default **Home** position refers to the center position defaulted in the factory. You might as well select another area of interest as the "Home" position. You should also select the speeds for the actions that occur during the patrol; i.e., pan, tilt, zoom, focus, and the auto pan/patrol.
2. Enter a name for a new preset position, which can contain up to forty characters. Click **Add** to enable the settings. The preset positions will be listed on the **User preset locations**. (To add positions you wish, please repeat steps 1~2.)
3. Select the preset positions and click on the **Save** button at the bottom of the screen.
4. Click on the move button (>>) >> to move positions to the Patrol locations window.
5. You may select some or all of the imported positions as the stop points during the tour.
6. Enter a preferred dwell time before the camera lens moves to the next position.
7. Select a **speed** level for the **auto patrol tour**.
8. Click on the **Save** button to preserve your configuration.

To remove a preset position from the list, select it and click **Remove**.
You can re-arrange the patrol order of the positions on the list using the ▲ ▼ buttons.

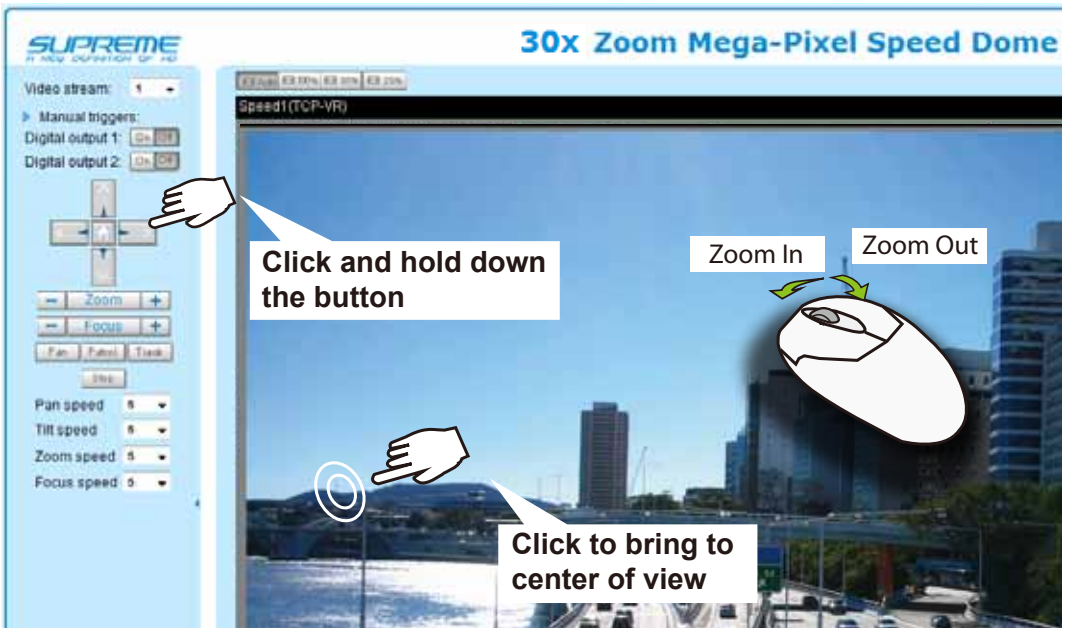
Misc. settings: Use the checkboxes and the pull-down menus for the camera to automatically resume the previous action or return to the home position after the camera has stayed idle for a period of time.



PTZ control panel operation mode: This determines how your mouse and PTZ control panel works on a live view window.



The **Continuous move** allows your screen control action to continue as long as you click and hold down the left mouse button. For example, if you click on the left button on the PTZ control panel, the camera's view should continuously rotate to the left until you release the button. The same applies to arrow keys, Zoom, and Focus buttons on the PTZ panel. If you select **Click to move**, every single mouse click takes effect for once without the ensuing move.



Note that if your screen control malfunctions, it is possible that the CPU of your current view station can not cope with the HD video feeds or that an incompatibility issue occurred with the ActiveX control plug-ins.

If you select the **Enable digital zoom** checkbox, you will be able to zoom in on an image by up to 360X magnification with the combination of the 30x mechanical zoom and another 12X digital zoom.

The **Enable Zoom enhancement** option takes effect only when a camera is showing a live stream of a smaller frame size, e.g., 640 x 360, than the maximum frame size. This option is enabled by default. This allows a slightly more zoom in ratio than the original mechanical zoom.

The **Zoom factor display:** This option is enabled by default, and zoom ratio is displayed along with the video title on the upper left corner of a view cell.

Apply previous action if the camera idles for __(1~999) seconds: You can assign an action to be taken when the camera sits idle for a configurable period time. For example, you can let camera resume a patrol tour. The resumed patrol will continue from the last preset position. You may also let the camera return to the home position. The idle state does not include the situations when the camera is performing pan or patrol action.

Return to home position: When no activities occur after a configurable period of time, let the camera's lens return to the default home position.

Positions on the Home page

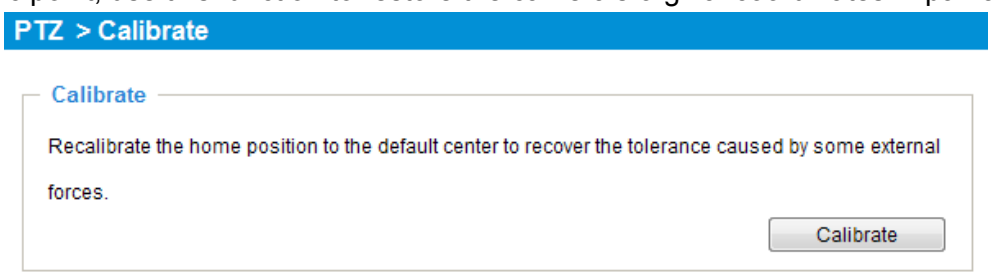
The **Preset positions** will also be displayed on the home page. Select one from the Go to drop-down list, and the Network Camera will move to the selected position.

Pan button: Click this button to start the 360° horizontal auto pan.

Patrol button: Click this button, then the Network Camera will patrol continuously among the selected positions.

PTZ > Calibrate

This function re-calibrates the home position to the default center to recover any displacement caused by external forces. Please note that there is no confirm message after using the function, and the calibration immediately takes place. If, after a long use, a user finds it is difficult to move camera's field of view to a specific point, use this function to restore the camera's orginal coordinates in pan and tilt motions.


PTZ > Calibrate
Calibrate
Recalibrate the home position to the default center to recover the tolerance caused by some external forces.
Calibrate

Auto tracking

In this window, you can modify the minimum object size as the triggering factor while performing the Auto Tracking function. You can move the camera view to an area of your interest, estimate, and define the possible size of objects. For example, you can designate the object size such as that of a human trespasser. The silhouette of the tresspasser must be larger than the whole of the object size square box. The minimum object size is 30x30 pixels within a 320x420 view window.

Use the slide bar to tune the sensitivity of the tracking function.

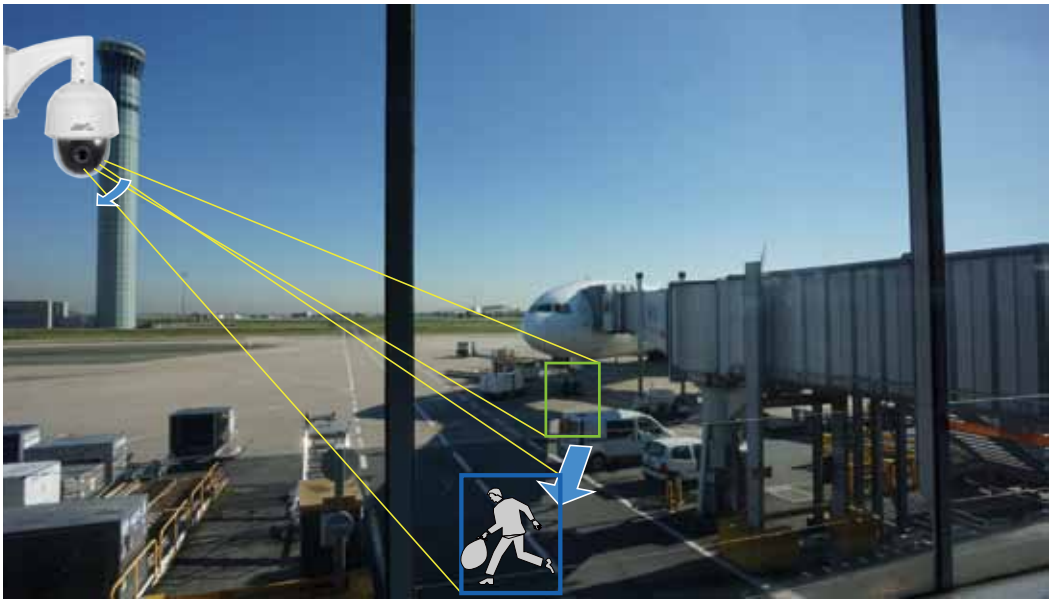
This function stops when the user clicks on any buttons on the PTZ panel, or a mouse click takes place on a view window.

Users can choose to perform other functions, such as pan or patrol, simply by clicking their buttons on the PTZ panel while the camera is performing the auto tracking function.

When Auto Tracking is taking place, a “Tracking” message is displayed on the message bar.

Auto tracking is configured by designating the minimum object size. Moving objects that entered the current region of view will trigger the tracking action.

Auto tracking, if applied, is designed to track an intruder in a place where human traffic is not heavy, such as a warehouse or a load area. Heavy traffic can result in a constant shift of tracked objects, and reduce the effectiveness of the feature.



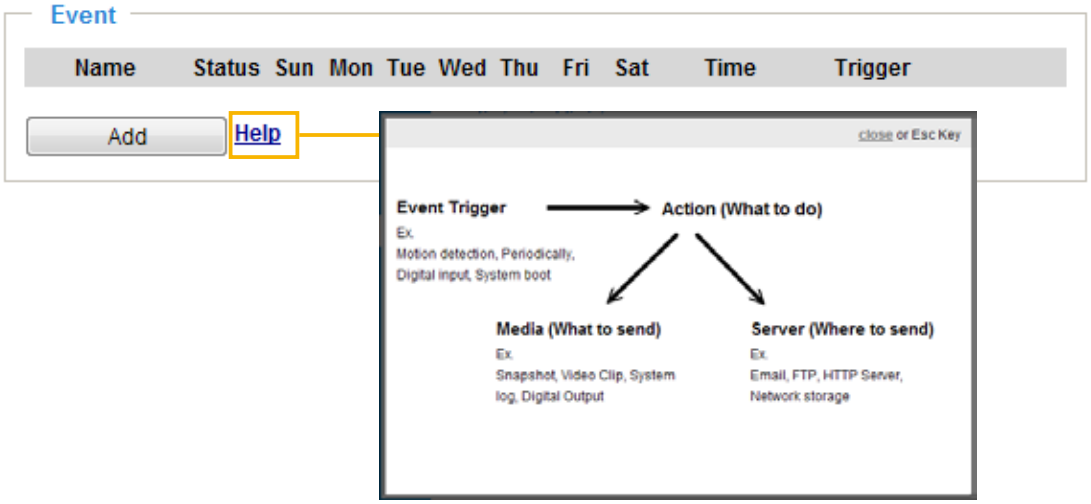
NOTE:

The conditions for using this function are listed below:

1. The speed dome can track one object at a time.
2. If multiple objects are present in the FOV, the camera tracks the object that is farthest from the camera.
3. If a tracked object stays motionless for 10 seconds, camera will abandon it and start tracking another object that is farthest away from the center.
4. The zoom-in ratio while tracking is determined by the zoom ratio of the camera lens when the tracking is triggered.
5. Manual control always has a higher priority than Auto tracking, such as using a joystick to pan or tilt or using a click on VAST view cell.
6. Objects can easily move away from an FOV when the zoom-in ratio is high. Therefore, it is recommended not to zoom in too much on where the Auto tracking is expected to take place.

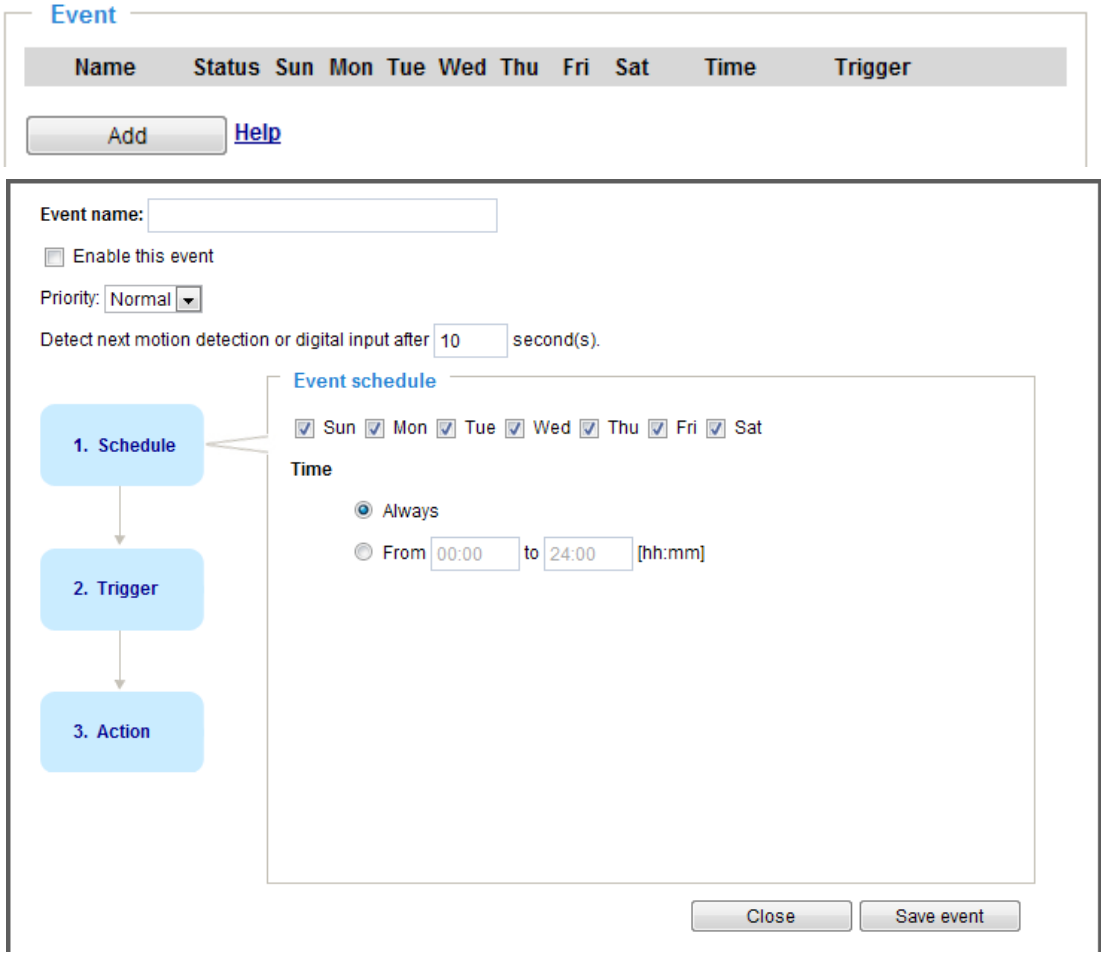
Event > Event settings

This section explains how to configure the Network Camera to responds to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action will be performed.



Event

An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window.



■ Event name: Enter a name for the event setting.

■ Enable this event: Select this option to enable the event setting.

■ Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

■ Detect next motion detection or digital input after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

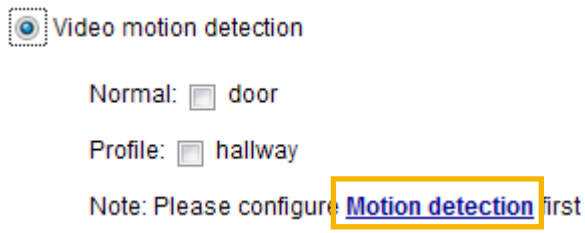
Follow the steps 1~3 to arrange the three elements -- Schedule, Trigger, and Action to configure an action to take when an event is triggered. You can configure 3 event-triggered conditions.

1. Schedule
Specify the time span for the event-triggering condition. Please select the days of the week and the time in a day (in 24-hr time format) for the recording schedule.

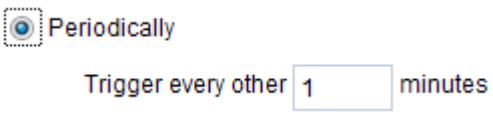
2. Trigger
This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

There are several choices of trigger sources as shown on next page. Select the item to display the detailed configuration options.

■ Video motion detection
This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 111 for details.



■ Periodically
This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.



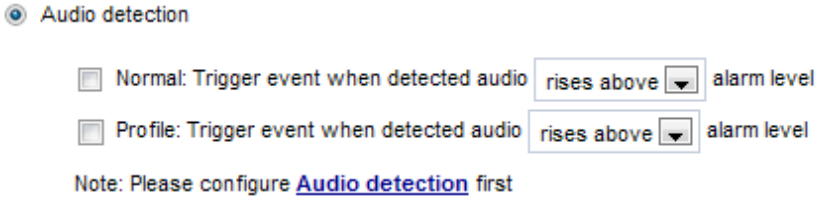
■ Digital input
This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

■ System boot
This option triggers the Network Camera when the power to the Network Camera is disconnected and reconnected.

■ Recording notify
This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data.

■ Audio detection

A preset threshold can be configured with an external microphone as the trigger to system event. The triggering condition can be an input exceeding or falling below a threshold. Audio detection can take place as a complement to motion detection or as a method to detect activities not covered by the camera's view. Please refer to page 114 **Applications** > **Audio detection** for more details.



Once you have a preset audio alarm level, you can define the triggering condition either as an audio input rises above or falls below the alarm level.

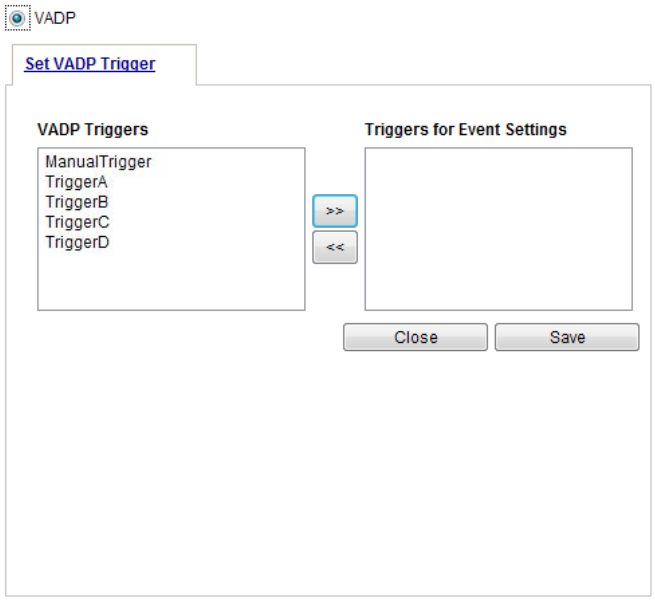
■ Manual triggers

An event can be manually triggered by the manual trigger buttons on the main page.

■ VADP

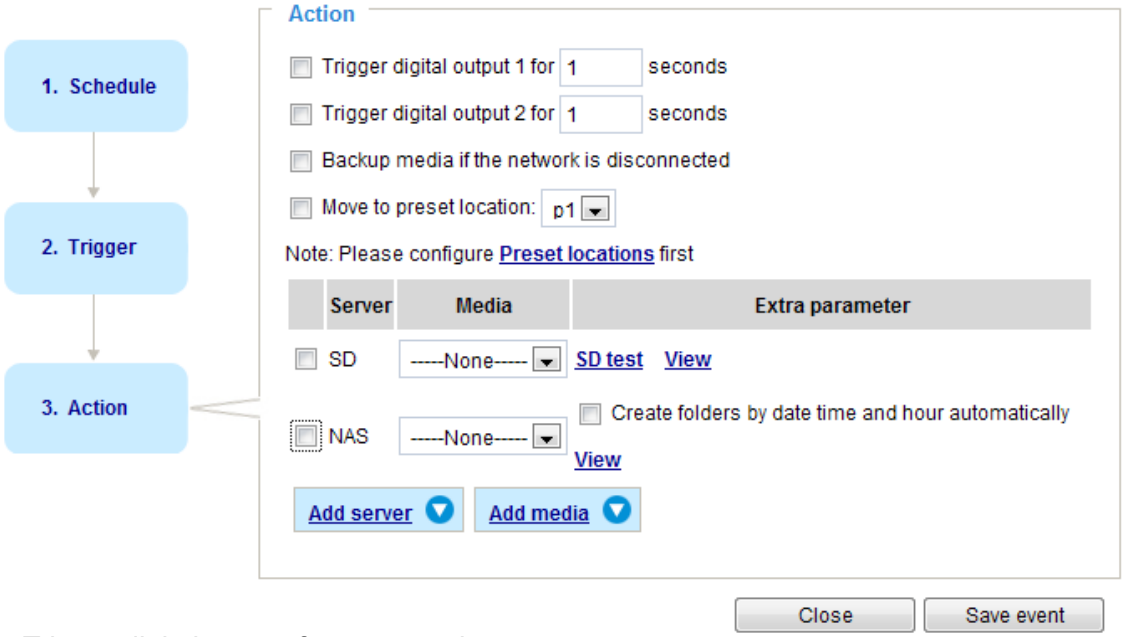
It is presumed that you already uploaded and enabled the VADP modules before you can associatee VADP triggers with an Event setting.

Click on the Set VADP Trigger button to open the VADP setup menu. The triggering conditions available with 3rd-party software modules known as VADP will be listed. Use the arrow buttons to select these triggers. Users may implant these modules for different purposes such as triggering motion detection, or applications related to video analysis, etc. Please refer to page 117 for the configuration options with VADP modules.



3. Action

Define the actions to be performed by the Network Camera when a trigger is activated.



■ Trigger digital output for ☐ seconds

Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

■ Backup media if the network is disconnected

Select this option to backup media file on SD card if the network is disconnected. Please note that this function will only be displayed after you set up a networked storage (NAS). For more information about how to set up network storage, please refer to page 121.

■ Move to preset location

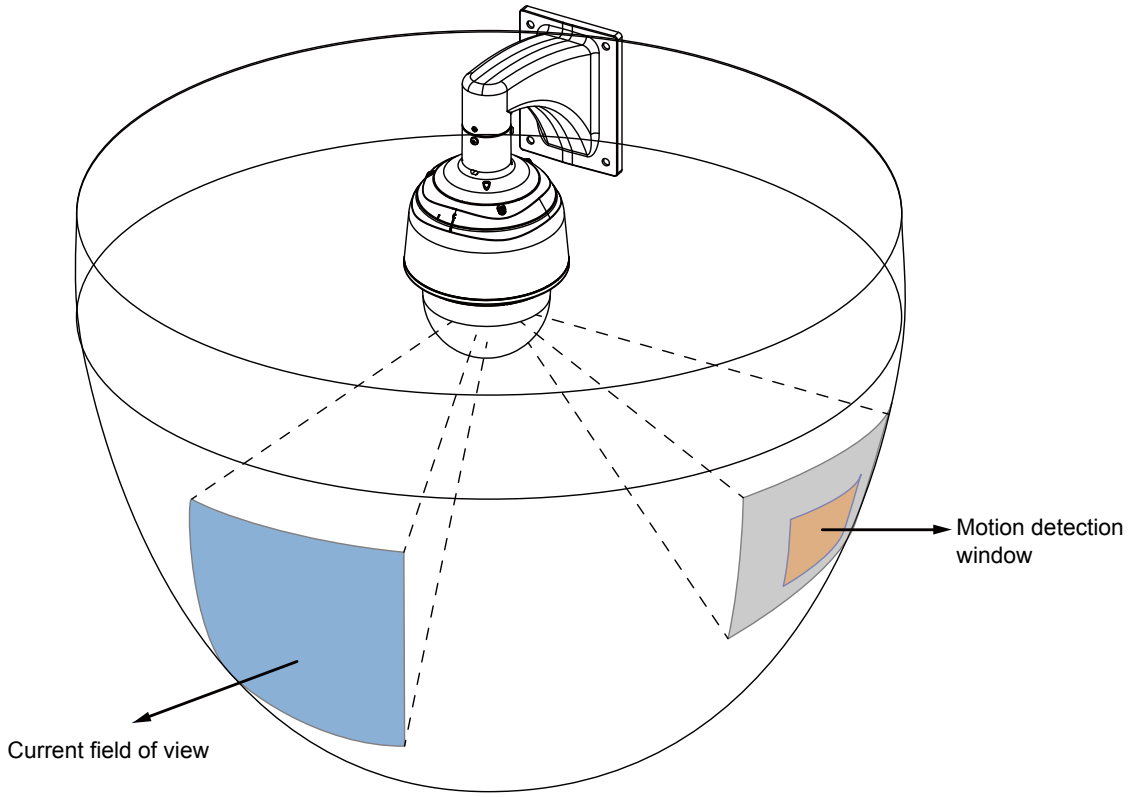
Select a preset location you've configured. Note that please configure **Preset locations** first. For detailed information, please refer to page 92. Another checkbox will appear, **Capture media after moving to the location**. You can select to record associated snapshot, video clip or system event once the event is triggered and the camera moves to the preset location. See Add Media in the following discussion.

To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated.

NOTE:

If you configured a motion detection window as a trigger, the motion detection may become invalid when the camera's field of view moved away from the detection window.

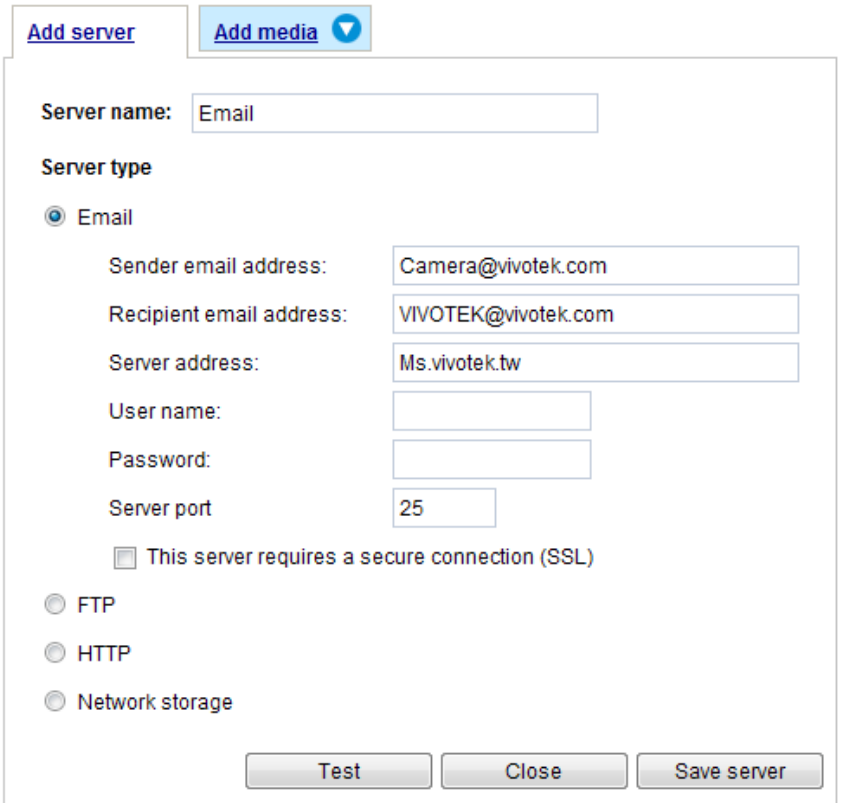
You can let camera return to the motion detection position to detect the coming event by re-configuring your Home position in **PTZ > PTZ settings** (see page 91) or turn the camera to a preset position.



Add server

Click **Add server** to unfold the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.



Server type - Email
Select to send the media files via email when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

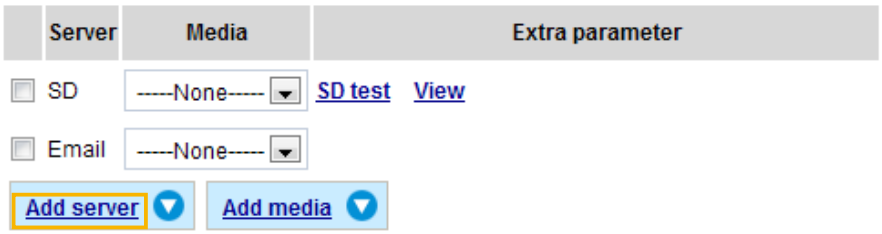
■ Server port: The default mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.

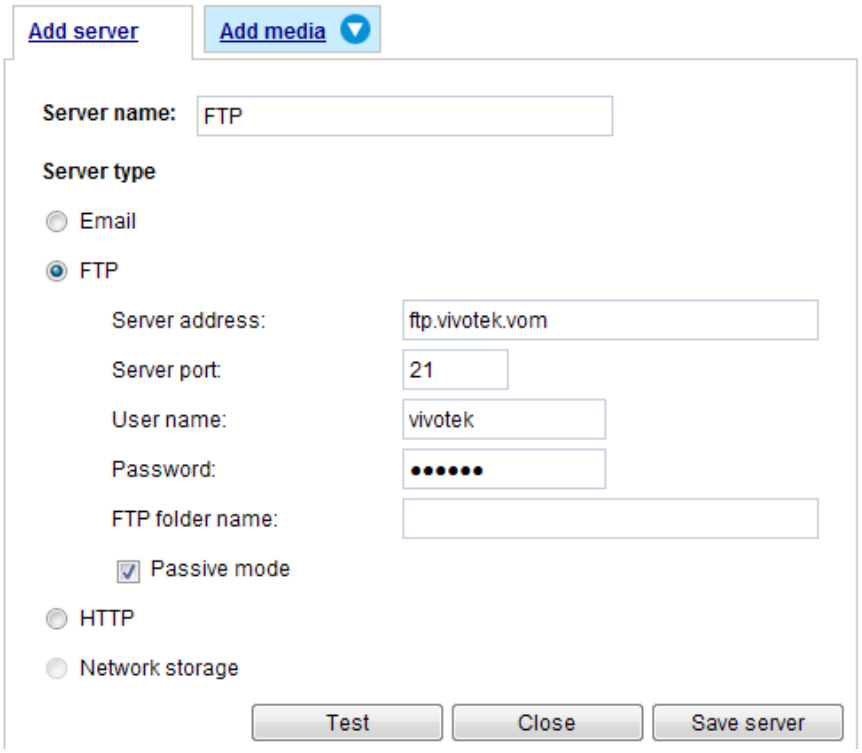
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

After you set up the first event server, a new item for event server will automatically show up on the Server list. If you wish to add more server options, click **Add server**.



Server type - FTP

Select to send the media files to an FTP server when a trigger is activated.



■ Server name: Enter a name for the server setting.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port: By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.

Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

Server type - HTTP
Select to send the media files to an HTTP server when a trigger is activated.

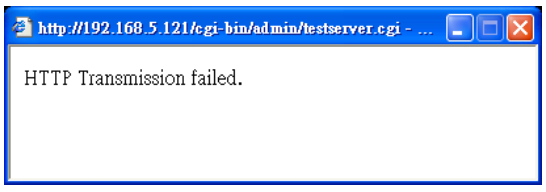
■ Server name: Enter a name for the server setting.

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

■ Password: Enter the password if necessary.

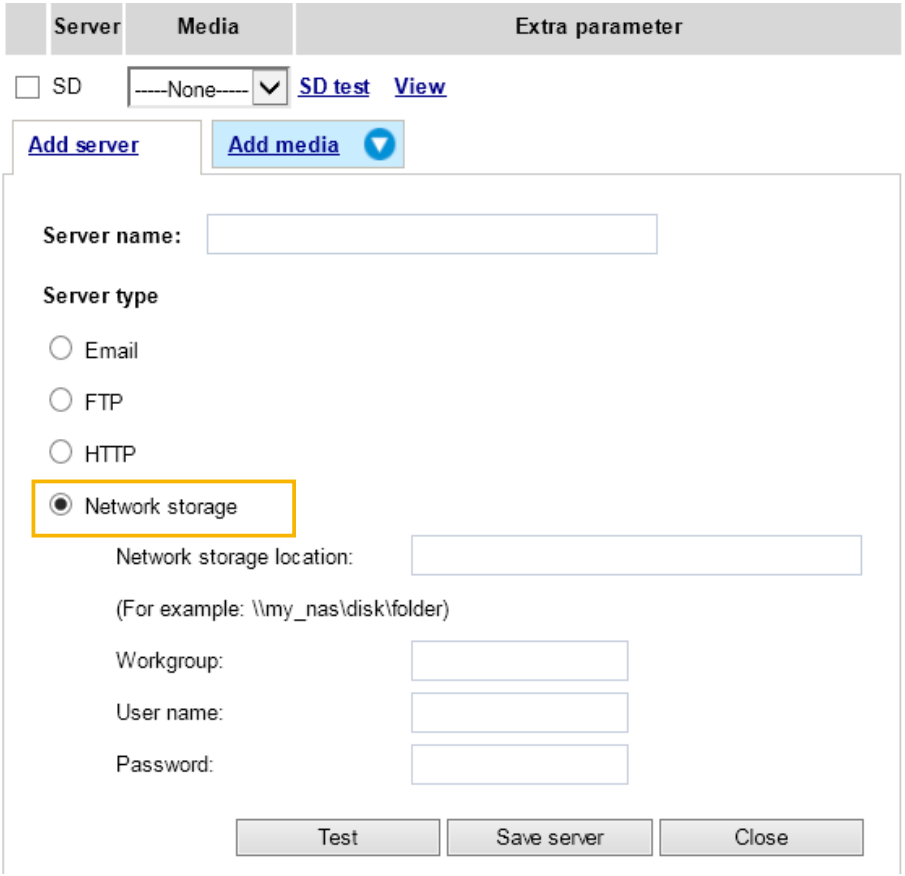
To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.



Click **Save server** to enable the settings and click **Close** to exit the Add server page.

Network storage:
Select to send the media files to a network storage location when a trigger is activated. Please refer to **NAS server** on page 121 for details.

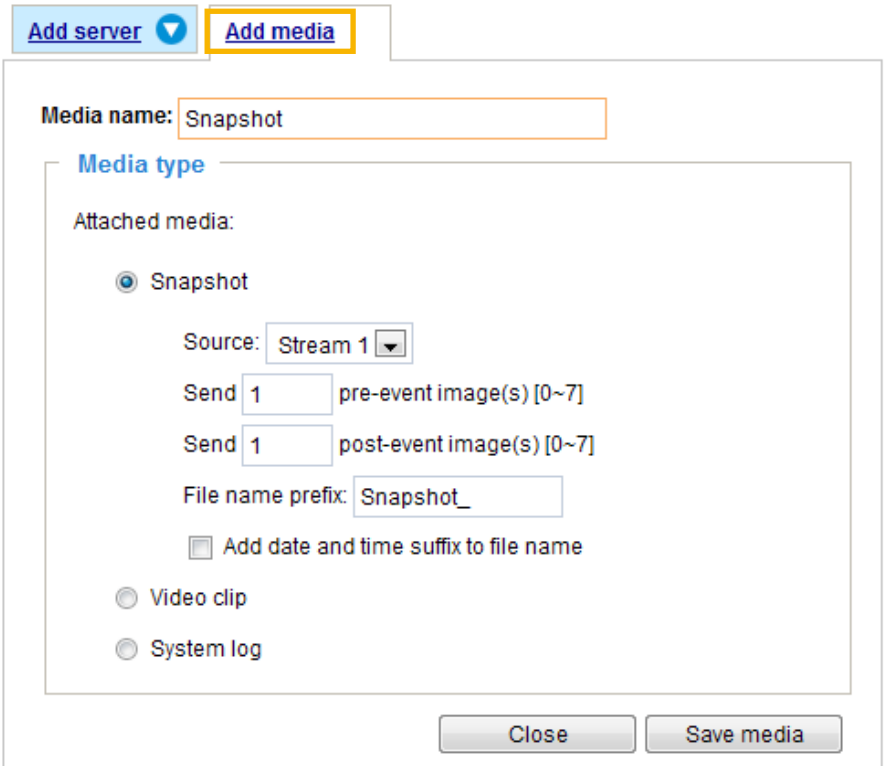
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.



- SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 124 for detailed information.

Add media

Click **Add media** to open the media setting window. You can specify the type of media that will be sent and preserved when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.



Media type - Snapshot
Select to send snapshots when a trigger is activated.

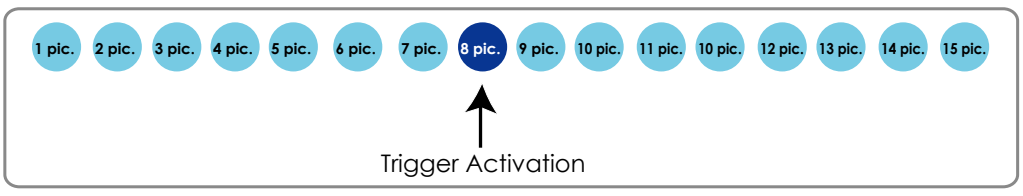
■ Media name: Enter a name for the media setting.

■ Source: Select to take snapshots from stream 1 ~ 4. (The following options are available when the check circle is selected.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

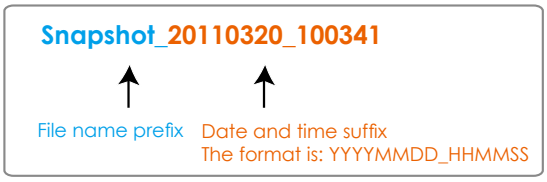
■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



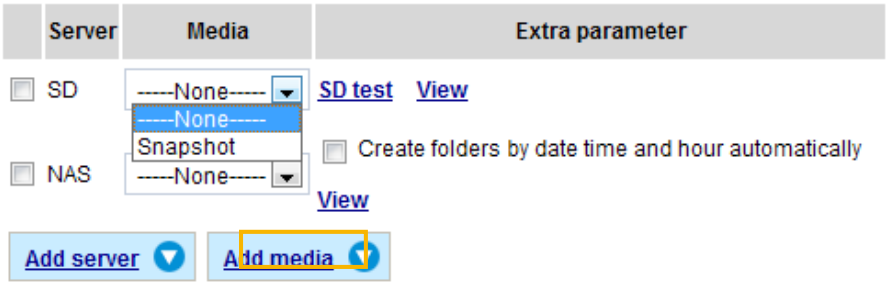
■ File name prefix
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:

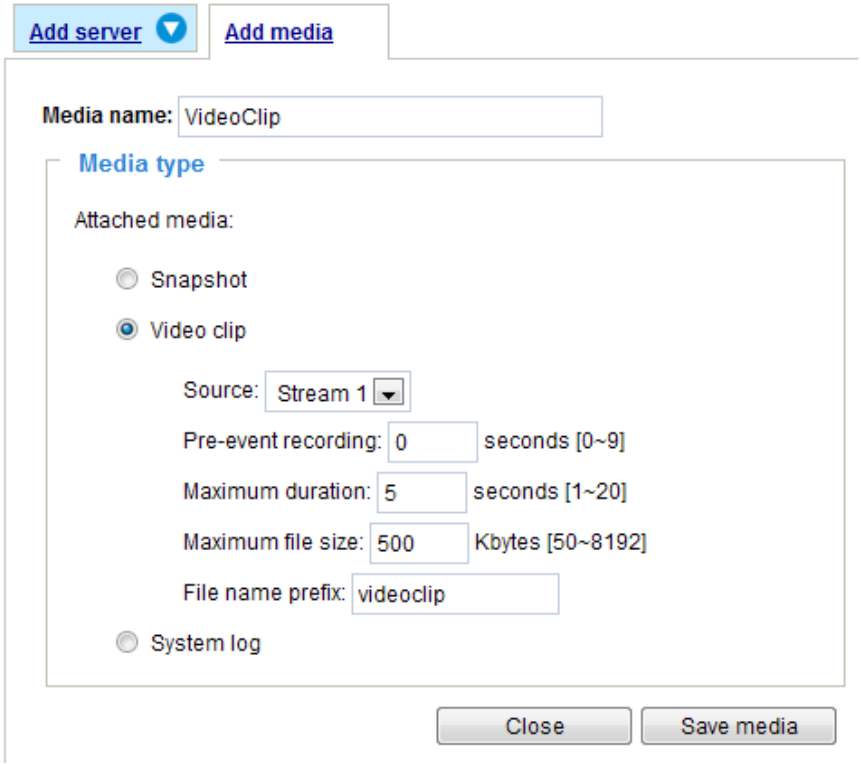


Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

After you set up the first media server, a drop-down menu of existing medias will be available on the Media list. If you wish to add more media options, click **Add media** again.



Media type - Video clip
Select to send video clips when a trigger is activated.

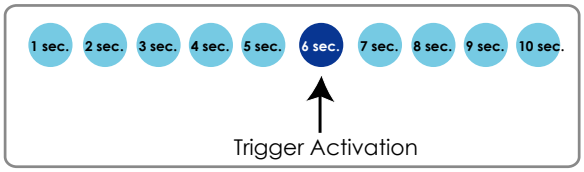


■ Media name: Enter a name for the media setting.

■ Source: Select the source of video clip.

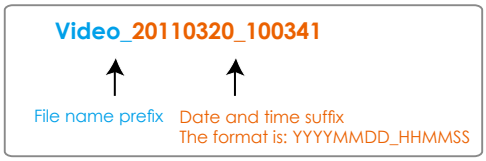
■ Pre-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 20 seconds can be set.
For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



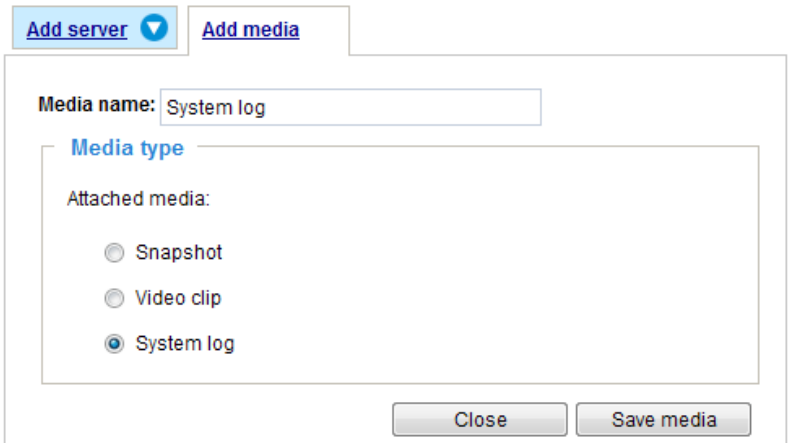
■ Maximum file size
Specify the maximum file size allowed.

■ File name prefix
Enter the text that will be appended to the front of the file name.
For example:

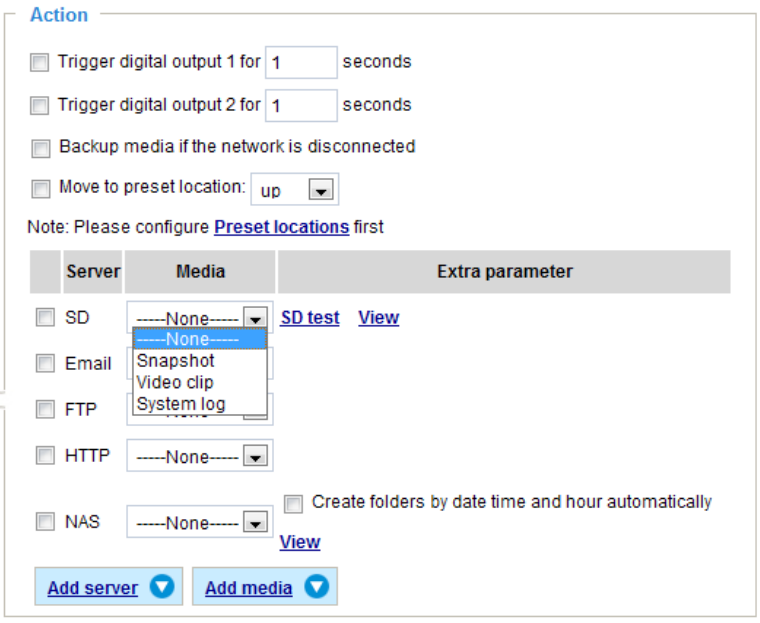


Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

Media type - System log
Select to send a system log when a trigger is activated.



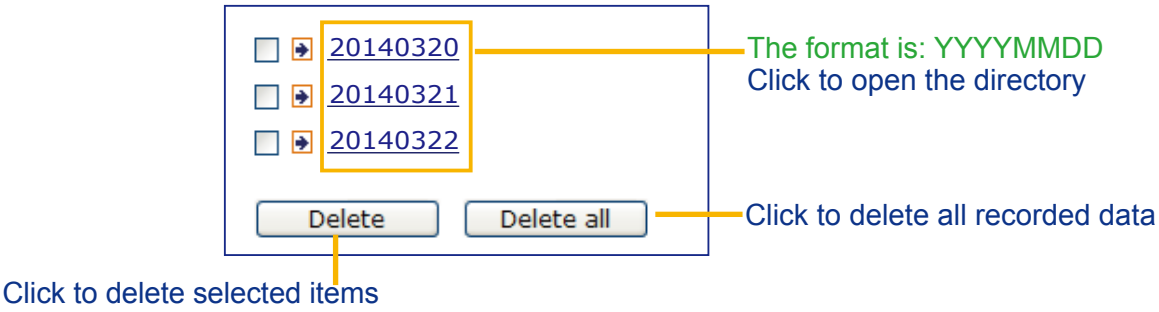
Click **Save media** to enable the settings, then click **Close** to exit the Add media page.



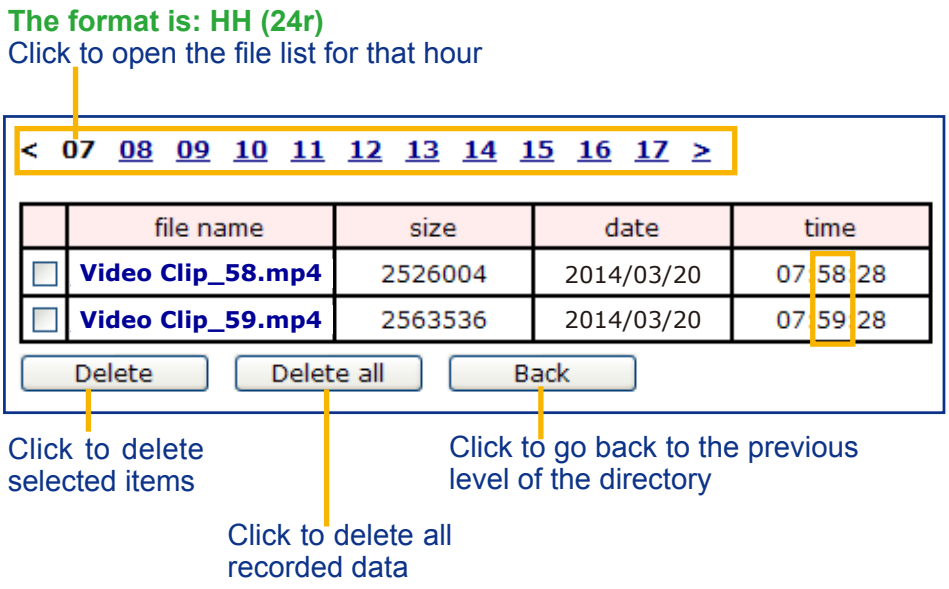
- View: Click this button to open a file list window. This function only apllies when an SD card and networked storage are available.
  If you click **View** button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 124. If you click **View** button of Network storage, a file directory window will pop up for you to view recorded data on Network storage.

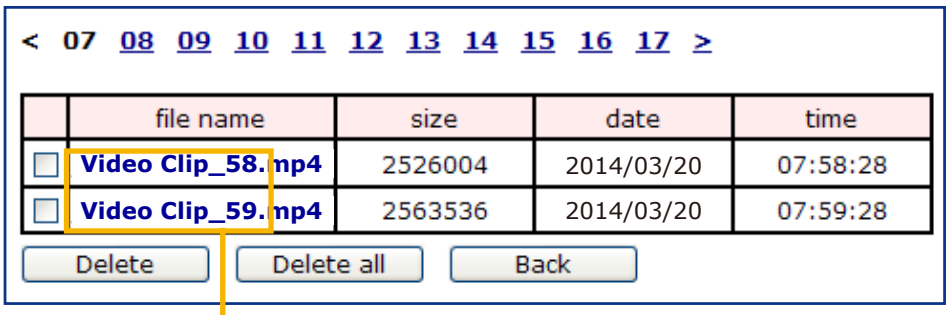
- Create folders by date, time, and hour automatically: If you check this item, the system will automatically create sub-folders named by the date.

The following is an example of a file destination with recorded video clips:

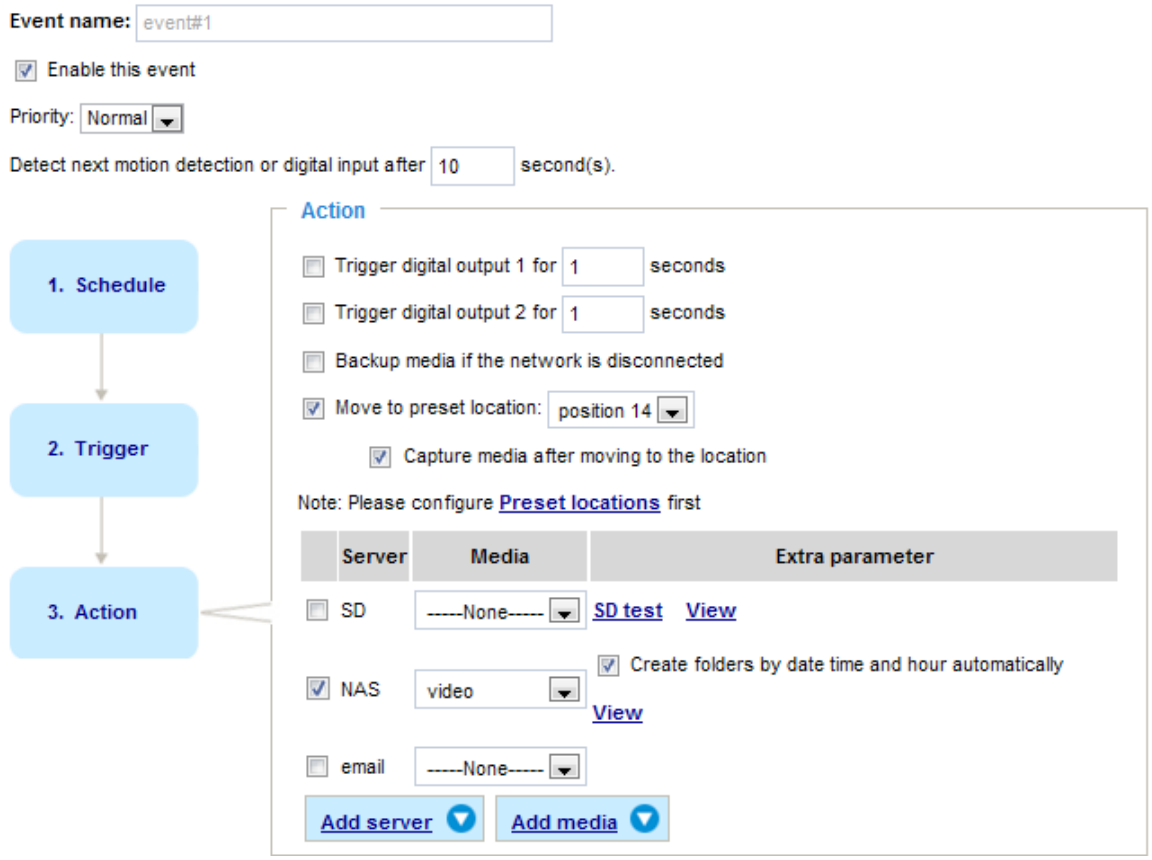


Click **20140320** to open the directory:



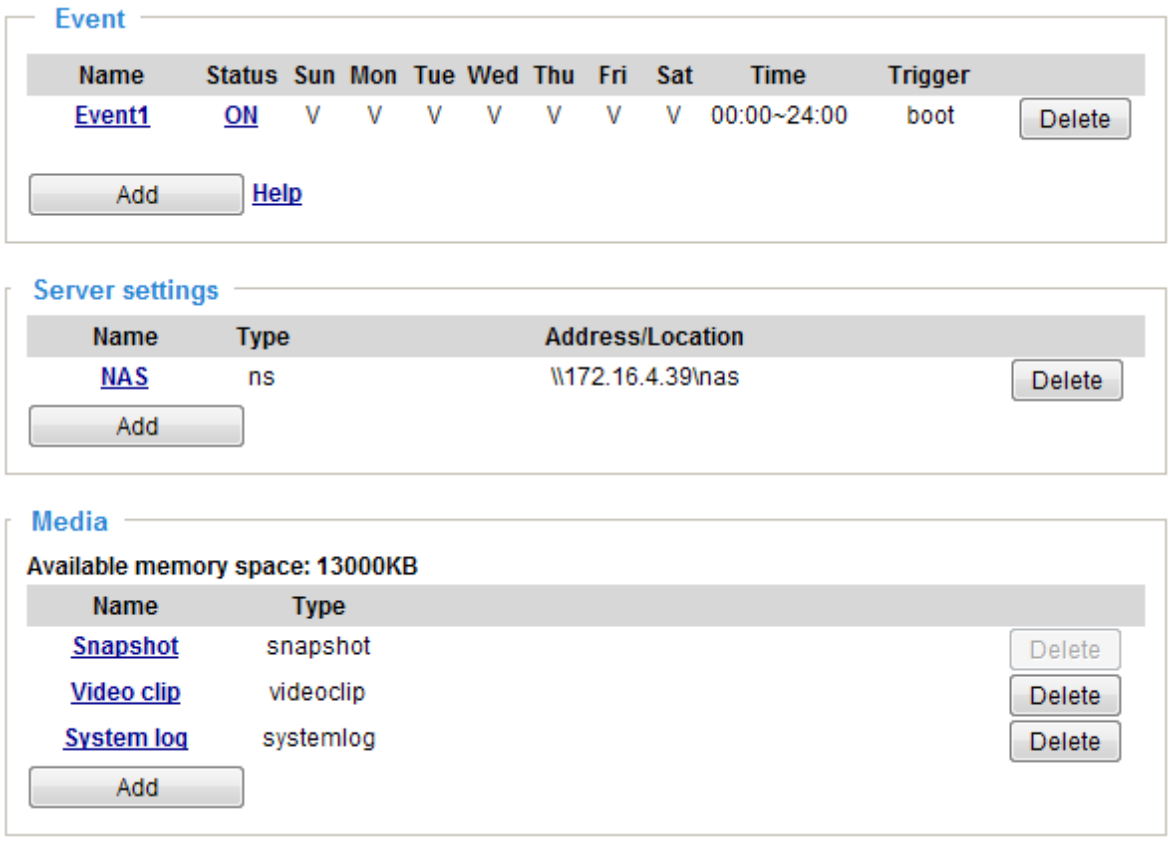


Here is an example of the Event setting:



When completed the settings with steps 1~3 to arrange Schedule, Trigger, and Action of an event, click **Save event** to enable the settings and click **Close** to exit the page.

The following is an example of the Event setting page:



When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mails.

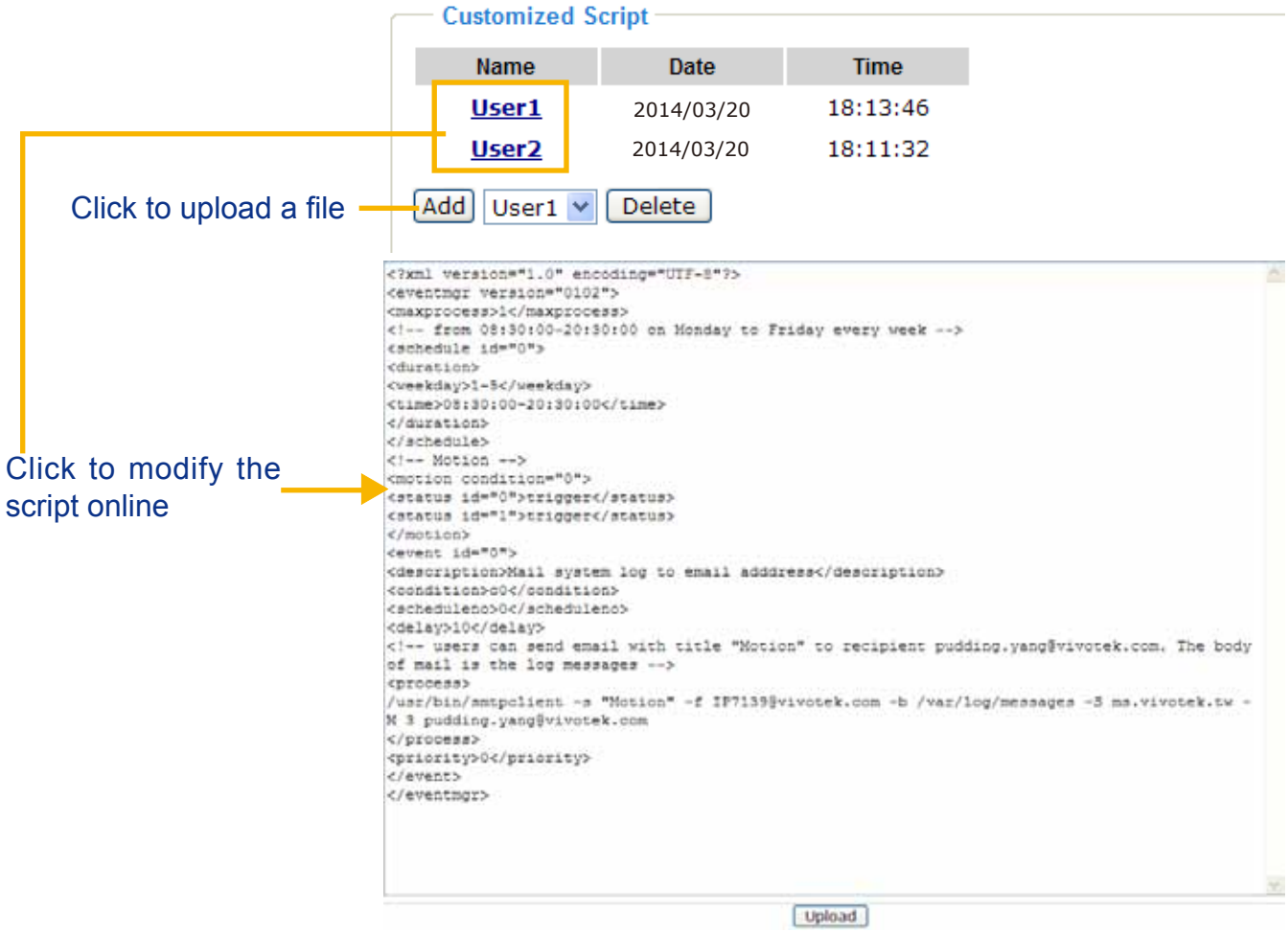
If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name and click **Delete**. Note that you can only delete a server setting when the server setting is currently not applied to an event setting.

To remove a media setting from the list, select a media name and click **Delete**. Note that you can only delete a media setting when the media setting is currently not applied to an event setting.

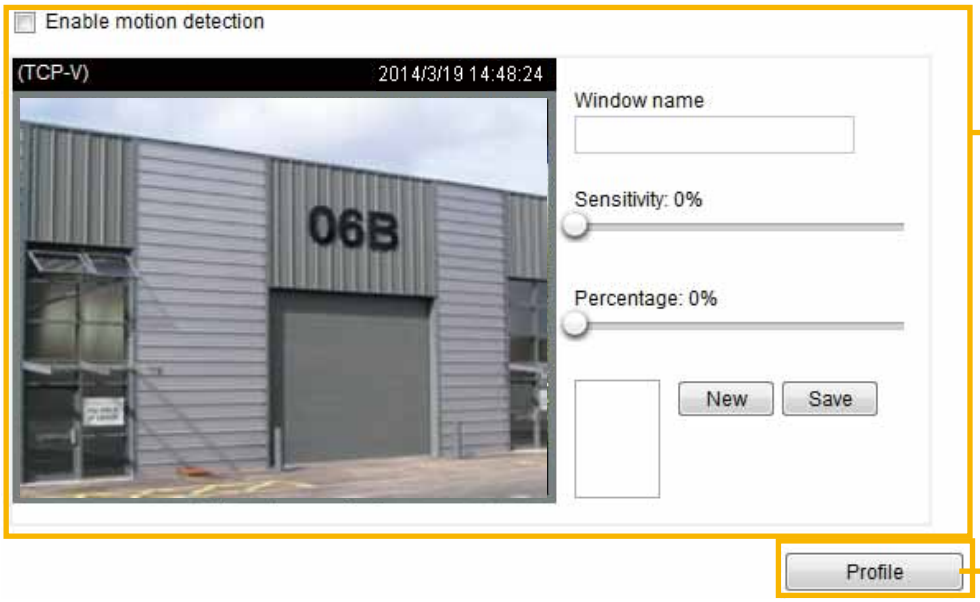
Customized Script

This function allows you to upload a sample script (.xml file) to the camera, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will prompt. If you need more information, please contact VIVOTEK technical support.



Applications > Motion detection

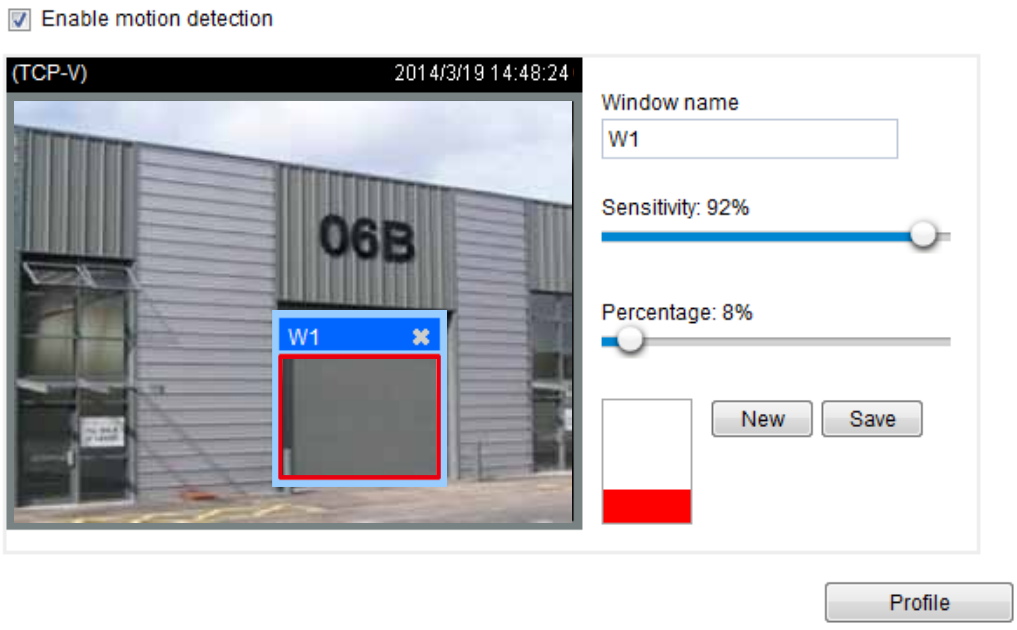
This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



Follow the steps below to enable motion detection:

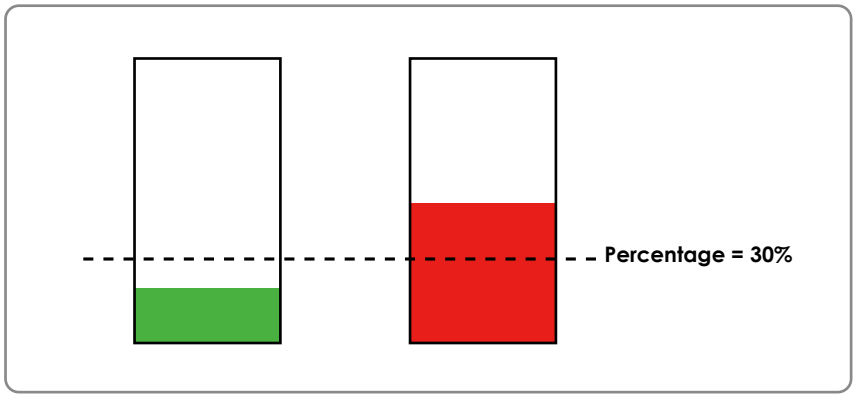
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   - To move and resize the window, drag and drop your mouse on the window.
   - To delete window, click X on the top right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:

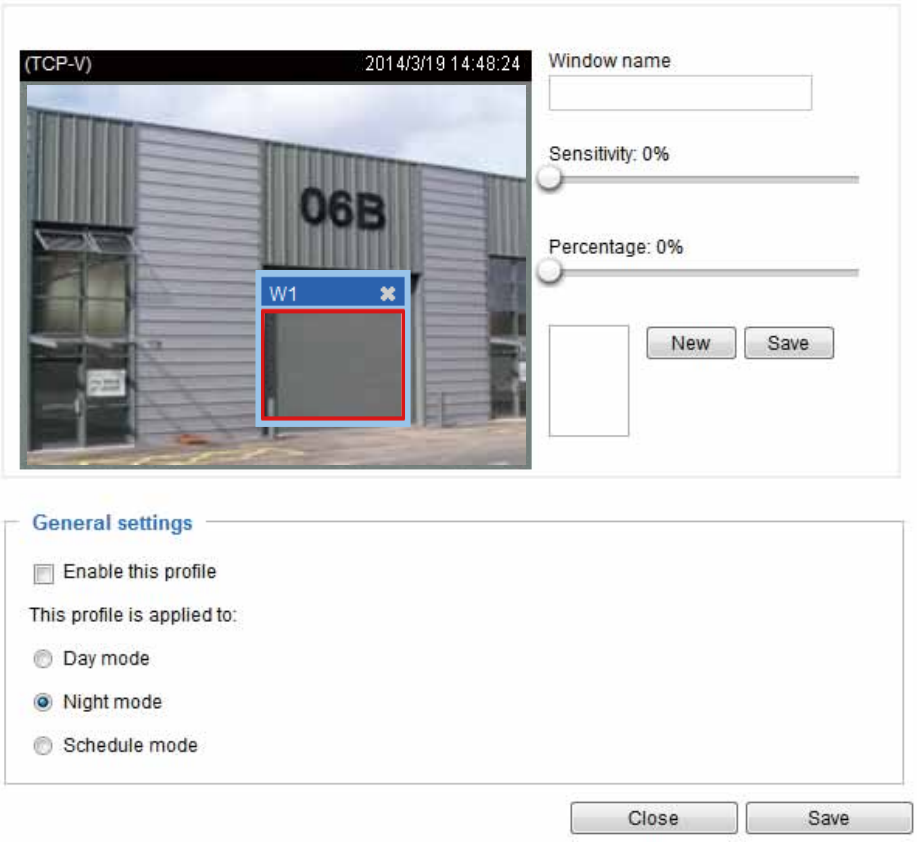


The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Event settings on page 96.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



If you want to configure other motion detection settings for day/night/schedule mode, please click **Profile** to open the Motion Detection Profile Settings page as shown below. A total of three motion detection windows can be configured on this page as well.

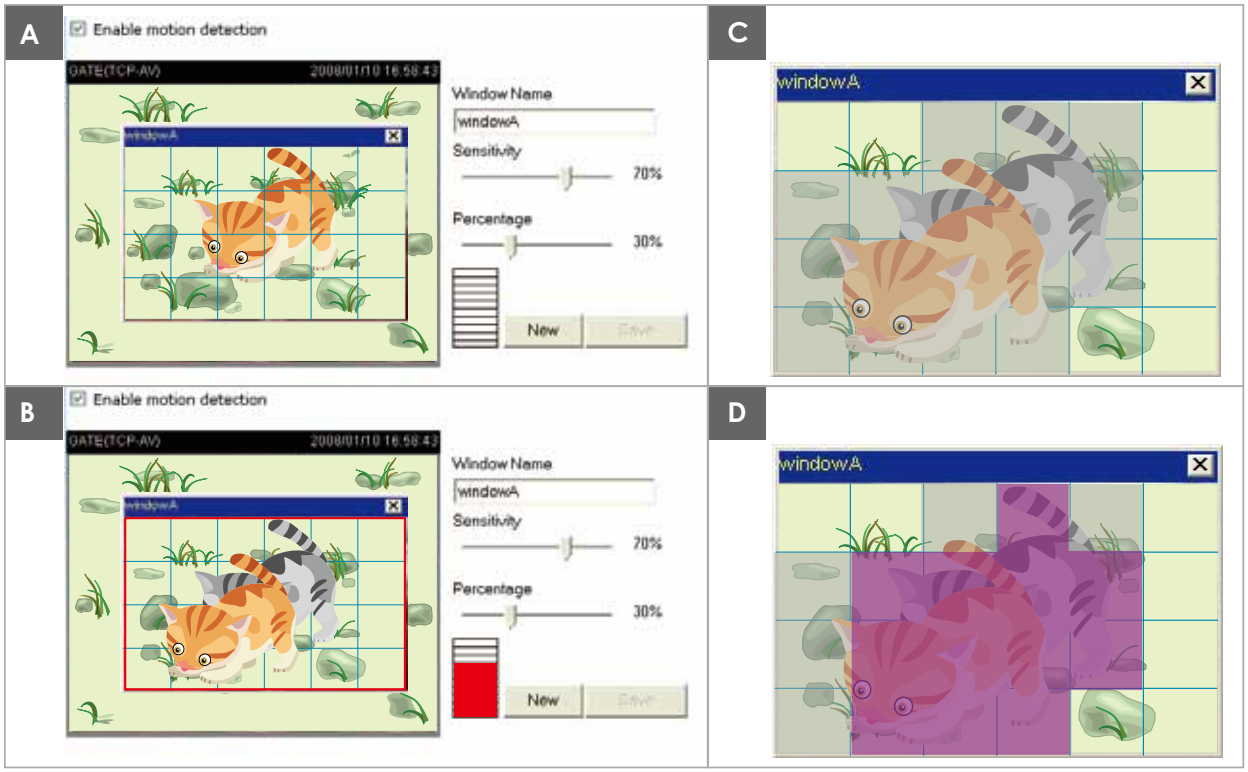


Please follow the steps beolw to set up a profile:
1. Create a new motion detection window.
2. Check **Enable this profile**.
3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you choose Schedule mode.
4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event settings page. You can go to Event > Event settings > Trigger to configure it as a trigger source. Please refer to page 97 for detailed information.

NOTE:

► *How does motion detection work?*



There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings and smaller percentage values.

Applications > DI and DO

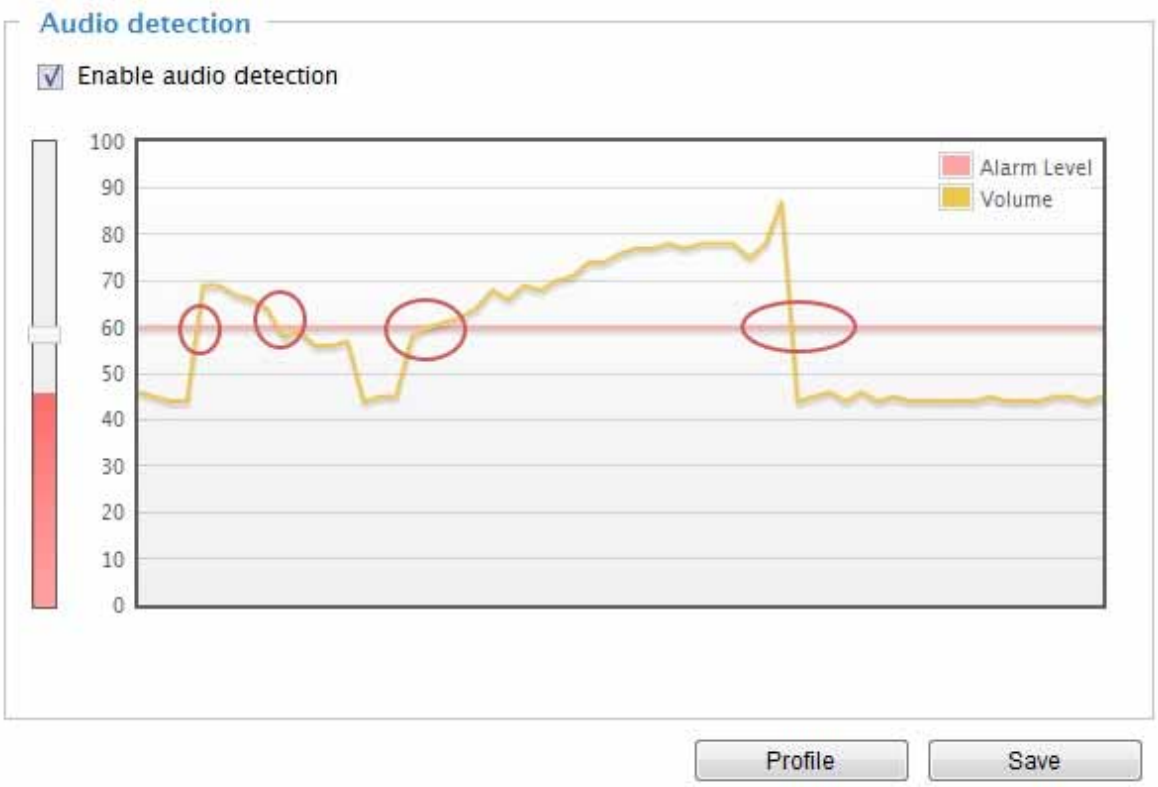
Digital input: Select High or Low to define normal status for the digital input. Connect a digital input from a sensor device to the camera, the Network Camera will report the current signal status. You may then configure the Normal status (non-trigger status) as High or Low.

Digital output: Select High or Low to define normal status for the digital output. Connect an output line to an external device, the Network Camera will report the current signal status. You may then configure the Normal status (non-trigger status) as High or Low.

Set up the event source as DI on **Event > Event settings > Trigger.** Please refer to page 97 for detailed information.

Applications > Audio detection

Audio detection, along with video motion detection, is applicable in the following scenarios:
1. Detection of activities not covered by camera view, e.g., a loud input by gun shots or breaking a door/ window.
2. A usually noisy environment, such as a factory, suddenly becomes quiet due to a breakdown of machines.
3. A PTZ camera can be directed to turn to a preset point by the occurrence of audio events.
4. Dark environments where video motion detection may not function well.



The red circles indicate where the audio alarms can be triggered when breaching or falling below the preset threshold.

How to configure Audio detection:
1. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.
2. Use a mouse click to drag the Alarm level tab to a preferred location on the slide bar.
3. Select the “Enable audio detection“ checkbox and click Save to enable the feature.

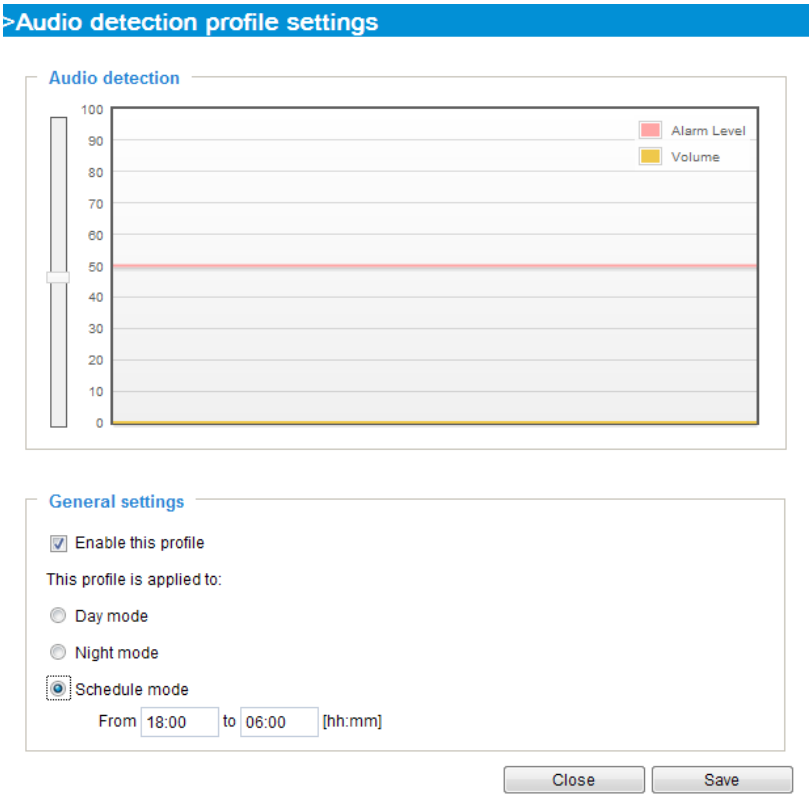
NOTE:

1. Note that the volume numbers (0~100) on the side of wave diagram does not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.

2. To configure this feature, you must not mute the audio in **Configuration > Media > Audio***. The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.*

You can use the **Profile** window to configure a different Audio detection setting. For example, a place can be noisy in the day time and become very quiet in the night.

1. Click on the **Enable this profile** checkbox. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.
2. Use a mouse click to drag the **Alarm level** tab to a preferred location on the slide bar.
3. Select the **Day**, **Night**, or **Schedule** mode check circles. You may also manually configure a period of time during which this profile will take effect.
4. Click **Save** and then click **Close** to complete your configuration.



IMPORTANT:

- If the Alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. It is recommended to set the Alarm level farther apart from the detected sound level.
- To configure and enable this feature, you must not configure video stream #1 into motion jpeg. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station along with stream #1.
- Refer to page 59 for Audio settings, and page 57 for video streaming settings.

Applications > VADP (VIVOTEK Application Development Platform)

Users can store and execute VIVOTEK's or 3rd-party software modules onto the camera's flash memory or SD card. These software modules can apply in video analysis for intelligent video applications such as license plate recognition, object counting, or as an agent for edge recording, etc.

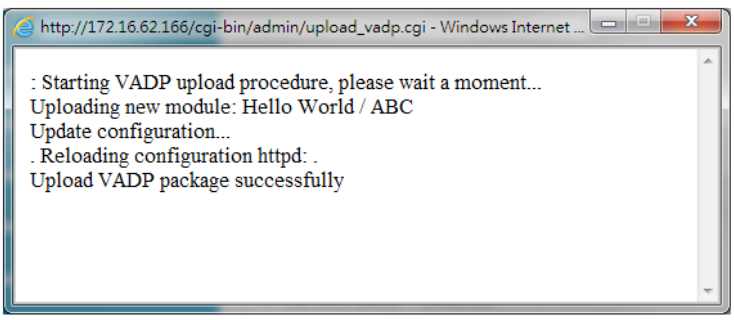
- Once the software package is successfully uploaded, the module configuration (vadp.xml) information is displayed. When uploading a module, the camera will examine whether the module fits the predefined VADP requirements. Please contact technical support or the vendor of your 3rd-party module for the parameters contained within.

- Users can also run VIVOTEK's VADP packages as a means to access updated functionality instead of replacing the entire firmware.

- Note that for some cameras the flash is too small to hold VADP packages. These cameras will have its "Save to SD card" checkbox selected and grayed-out for all time.

- The file system of SD card (FAT32) does not support soft (symbolic) link. It will return failure if your module tries to create soft links on SD card.

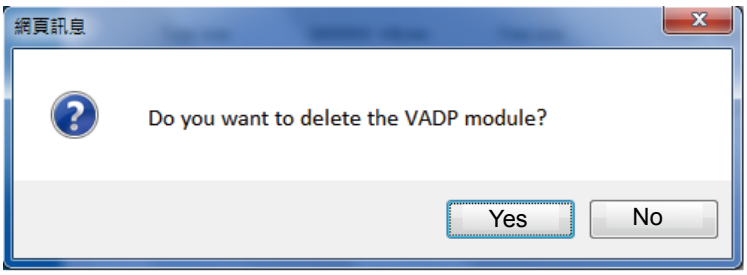
To utilize a software module, acquire the software package and click **Browse** and **Upload** buttons. The screen message for a successful upload is shown below:


http://172.16.62.166/cgi-bin/admin/upload_vadp.cgi - Windows Internet ...
: Starting VADP upload procedure, please wait a moment...
Uploading new module: Hello World / ABC
Update configuration...
. Reloading configuration httpd: .
Upload VADP package successfully

To start a module, select the checkcircle in front, and click the **Start** button.

If you should need to remove a module, select the checkcircle in front and then click the **Stop** button. By then the module status will become **OFF**, and the **X** button will appear at the end of the row. Click on the **X** button to remove an existing module.

When prompted by a confirm message, Click **Yes** to proceed.

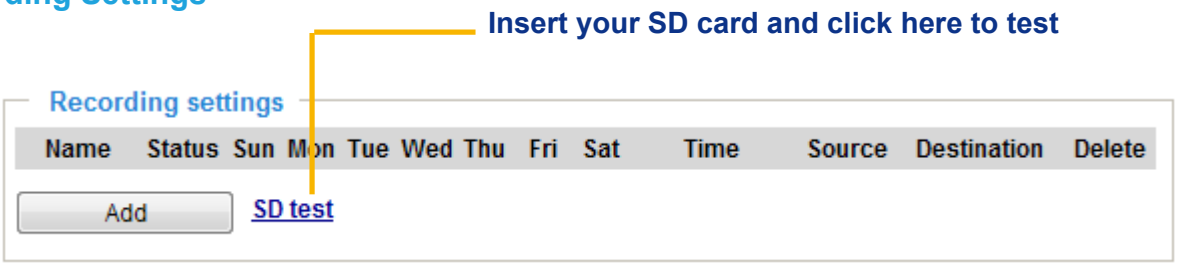


Note that the actual memory consumed while operating the module will be indicated on the **Memory status** field. This helps determine whether a running module has consumed too much of system resources.

Recording > Recording settings

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

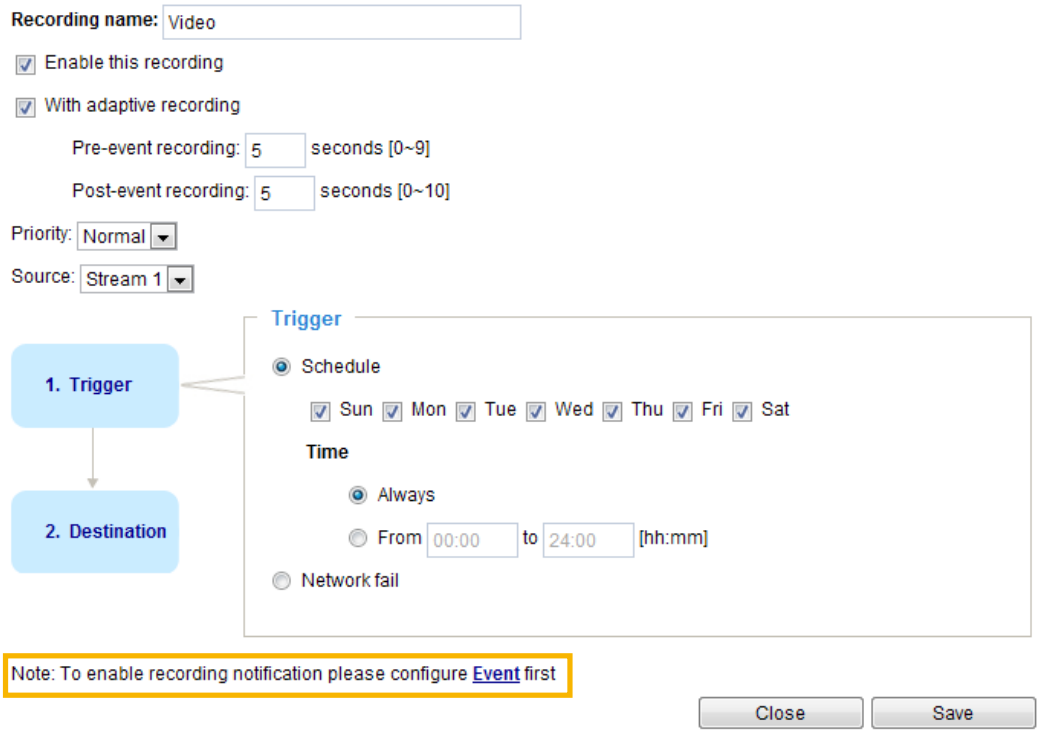

Insert your SD card and click here to test
Recording settings
Name Status Sun Mon Tue Wed Thu Fri Sat Time Source Destination Delete
Add
SD test

NOTE:

► *Please remember to format your SD card when using it for the first time. Please refer to page 124 for detailed information.*

Recording Settings

Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.

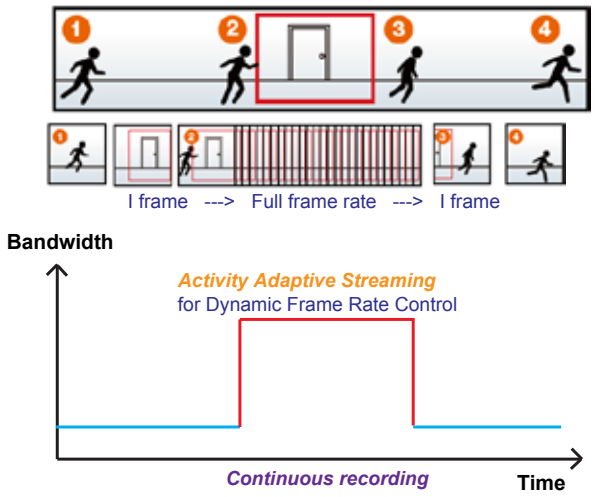


■ Recording name: Enter a name for the recording setting.

■ Enable this recording: Select this option to enable video recording.

■ With adaptive recording:
Select this option will activate the frame rate control according to alarm trigger. The frame control means that when there is alarm trigger, the frame rate will raise up to the value you've set on Stream setting page. Please refer to page 58 for more information.

If you enable adaptive recording and enable time-shift cache stream on Camera A, only when an event is triggered on Camera A will the server record video streams in the full frame rate; otherwise, it will only request the I frame data during normal monitoring, thus effectively save lots of bandwidth and storage.



NOTE:

► *To enable adaptive recording, please make sure you've set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.*

► *When there is no alarm trigger:*
- JPEG mode: record 1 frame per second.
- H.264 mode: record I frame only.
- MPEG-4 mode: record I frame only.

► *When the I frame period is >1s on Video settings page, it should be forced to make the I frame period to 1s when adaptive recording is activated.*

The alarm trigger includes: motion detection and DI detection. Please refer to Event settings on page 96.

■ Pre-event recording and post-event recording
The Network Camera has a buffer area; it temporarily holds data for up to a certain limit. Enter a number to decide the duration of recording that will take place before and after a trigger is activated.

■ Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.

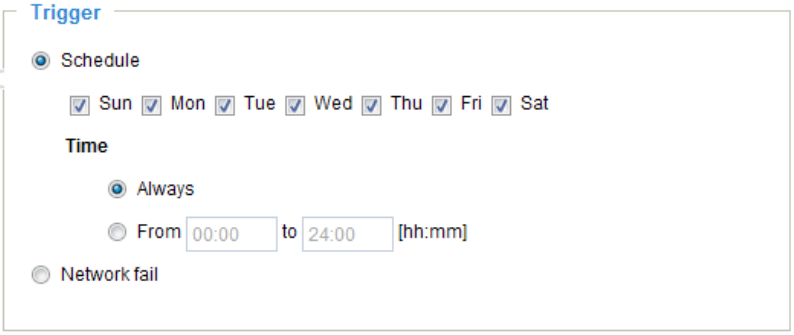
■ Source: Select a stream as the recording source.

NOTE:

► *To enable recording notification, please configure **Event settings** first. Please refer to page 96.*

Please follow steps 1~2 below to set up the recording:

1. Trigger
Select a trigger source.

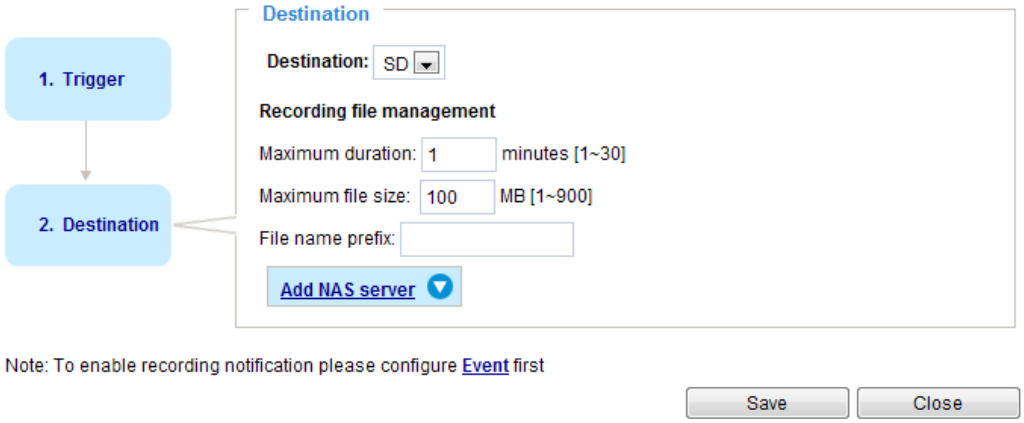


■ Schedule: The server will start to record files on the local storage or to a networked storage device (NAS).

■ Network fail: Since the time when the network fails, the server will start to record files on the local storage (SD card).

2. Destination

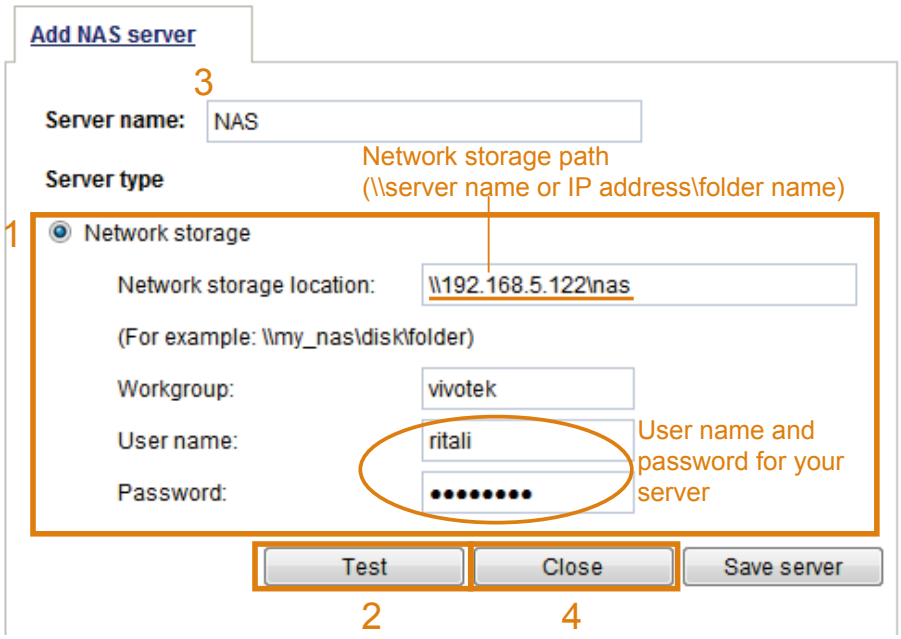
You can select the SD card or network attached storage (NAS) for recording video files.



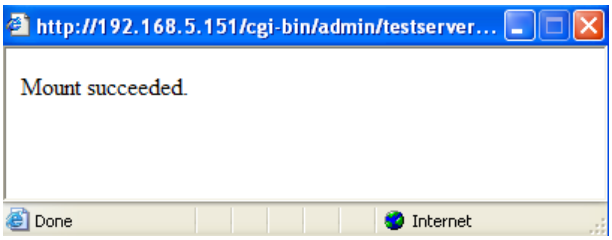
NAS server

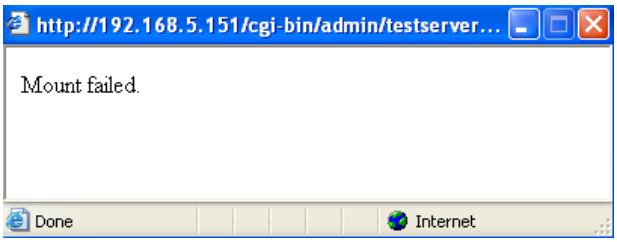
Click **Add NAS server** to open the server setting window and follow the steps below to set up:

1. Fill in the information for your server.
   For example:

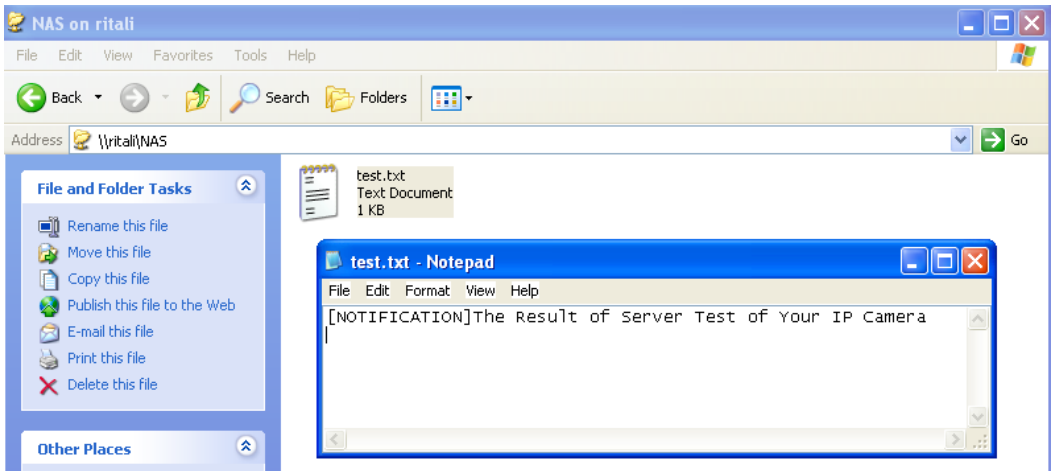


2. Click **Test** to check the setting. The result will be shown in the pop-up window.

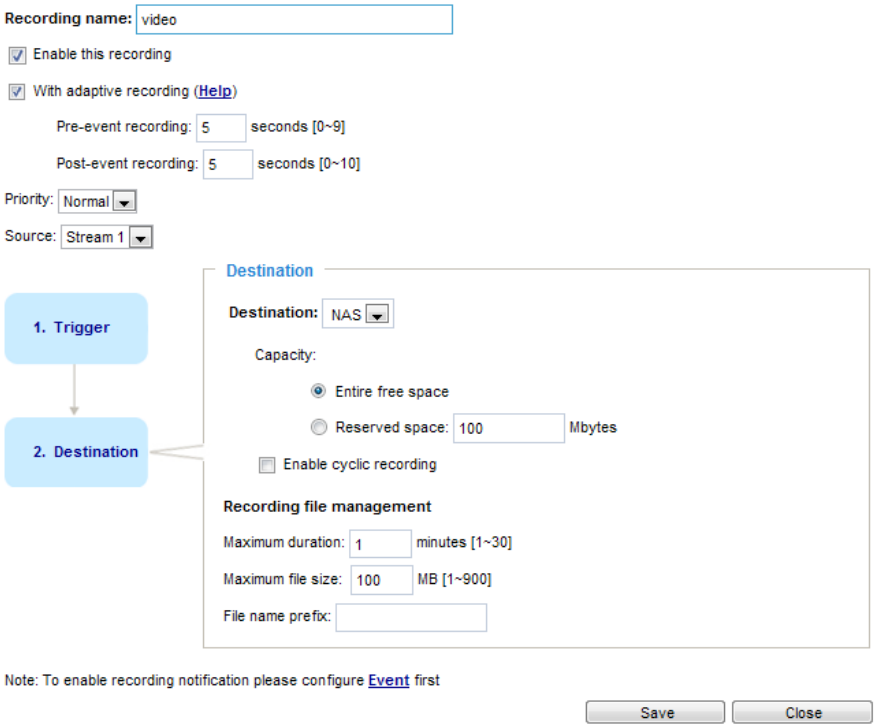




If successful, you will receive a test.txt file on the network storage server.



3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.



- Capacity: You can select either the entire storage space available or specify a reserved space. The recording size limit must be larger than the reserved space for cyclic recording. The reserved space is used during cyclic recording to prevent malfunctions that might occur during the transaction stage when the video feeds are about to fill up the storage space, and new data is still coming. This value must be larger than 15 MBytes.

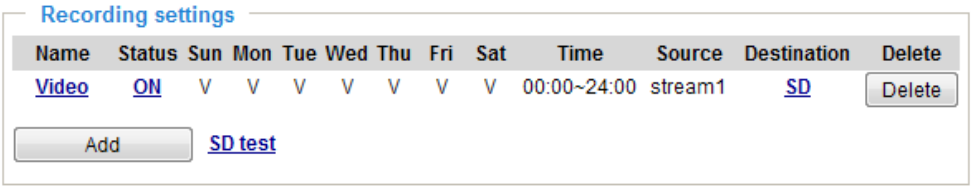
- Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest files will be overwritten by the latest ones.

- File name prefix: Enter the text that will be appended to the front of the file name.

If you want to enable recording notification, please click **Event** to set up. Please refer to **Event > Event settings** on page 96 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit

this page. When the system begins recording, it will send the recorded files to a networked storage or SD card. The new recording name will appear on the recording page as shown below.
To remove a recording setting from the list, select it and click **Delete**.


Recording settings
Name Status Sun Mon Tue Wed Thu Fri Sat Time Source Destination Delete
Video ON V V V V V V V 00:00~24:00 stream1 SD Delete
Add
SD test

■ **Video (Name)**: Click to open the Recording settings page to modify its details.

■ **ON (Status)**: Click to manually adjust the Status. (**ON**: start recording; **OFF**: stop recording)

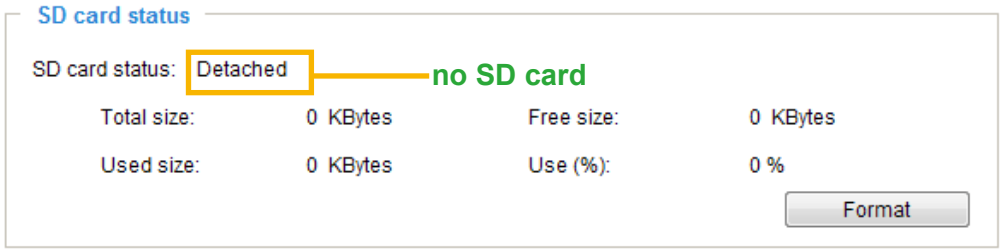
■ **NAS or SD (Destination)**: Click to open the file list of recordings as shown below. For more information about folder naming rules, please refer to page 108 or page 115 for details.

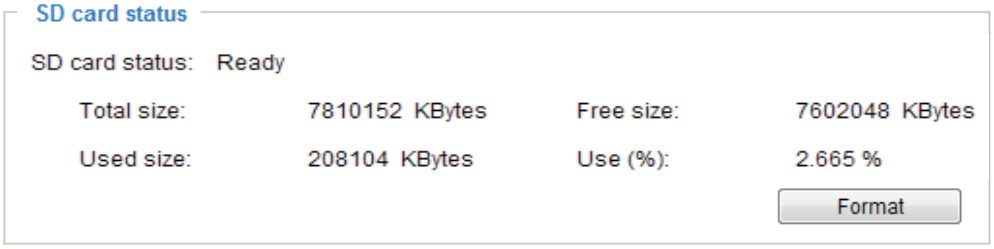
Local storage > SD card management

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

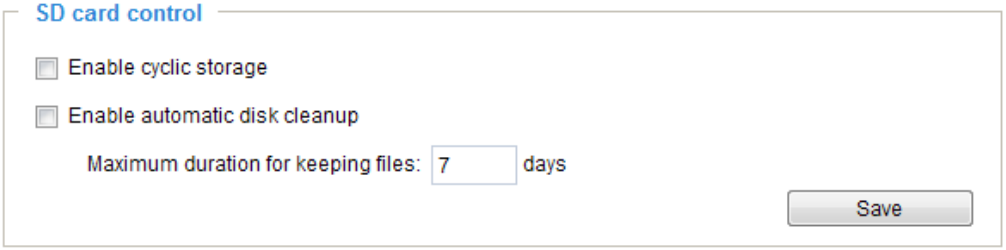
SD card status

This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.





SD card control



- Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest files will be overwritten by the latest ones.
- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

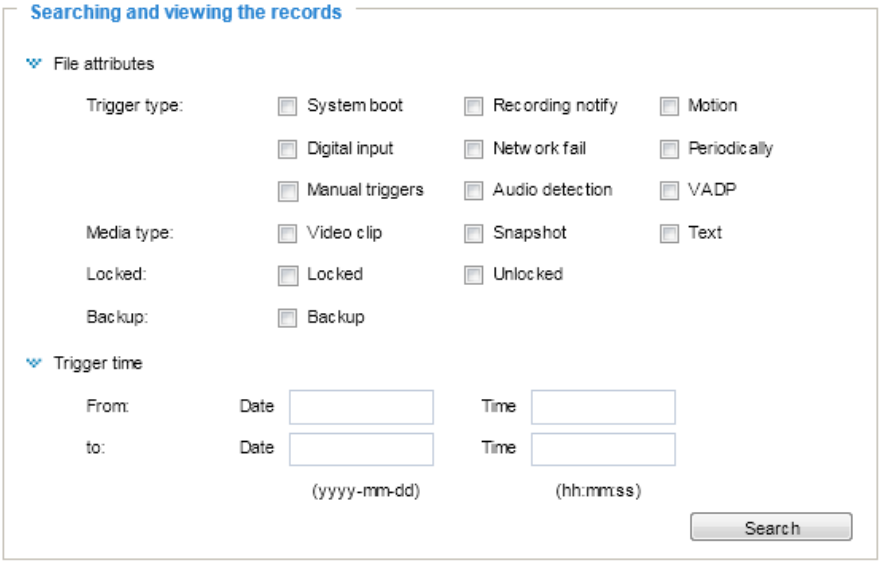
When all settings are completed, click **Save** to enable your settings.

Local storage > Content management

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the search results.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** column.

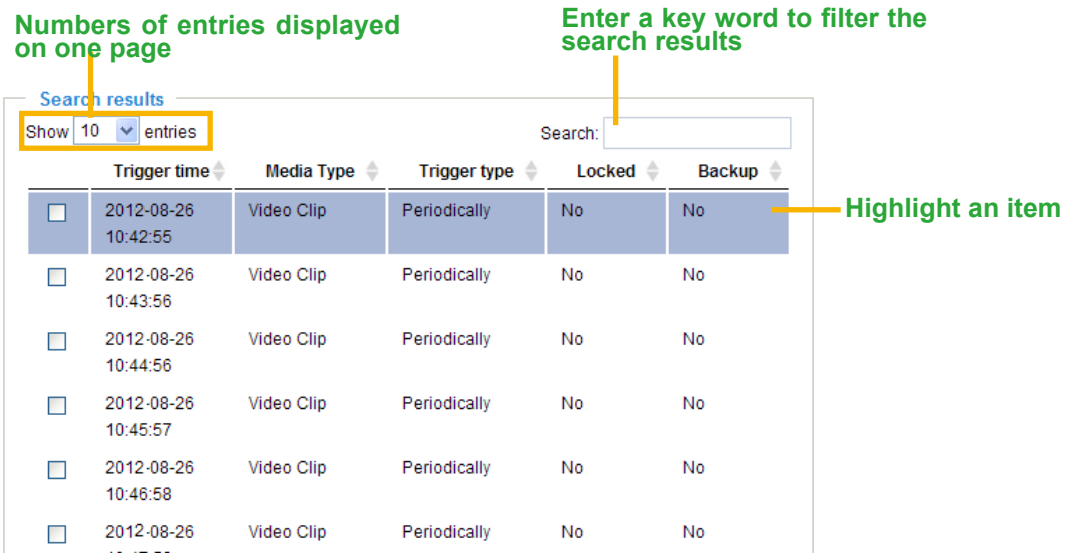


■ File attributes: Select one or more items as your search criteria.
■ Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data that matches the search criteria will be listed in **Search Results** window.

Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ⇕ to sort the search results in either direction.

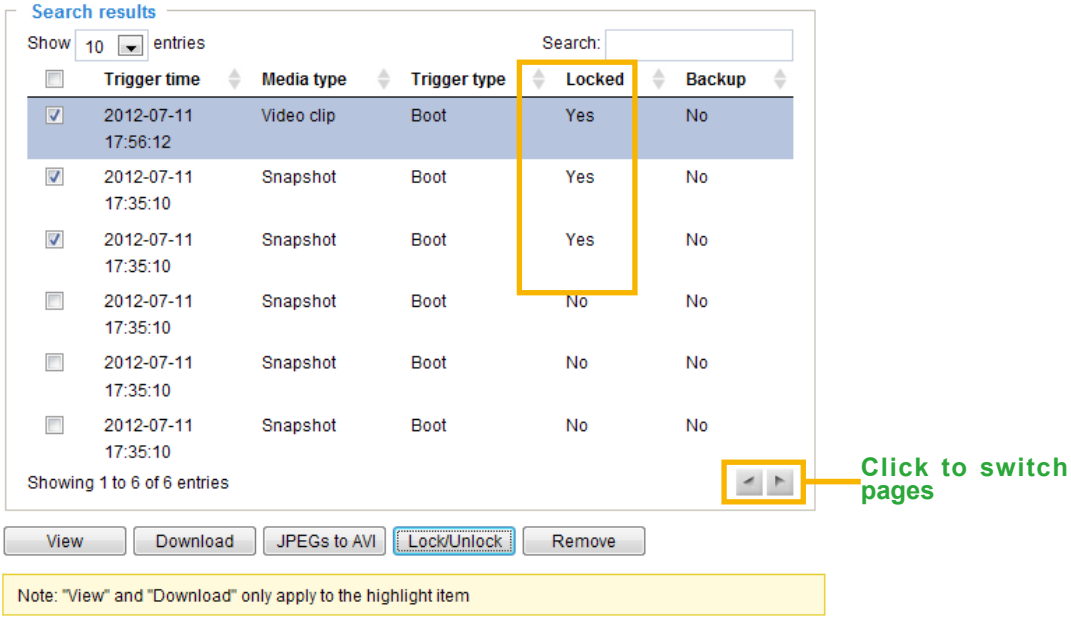


■ View: Click on a search result. The entry will be highlighted in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file.
For example:

■ Download: Click on a search result to select an entry as shown above. Then click the **Download** button and a file download window will prompt for you to save the file.

■ JPEGs to AVI: This function only applies to “JPEG“ format files such as snapshots. You can select several snapshots from the list, then click this button. The series of snapshots will be converted into an AVI file.

■ Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections.
For example:



■ Remove: Select the desired search results, then click this button to delete the files.

Appendix

URL Commands for the Network Camera

1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

2. Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

3. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*>
[?<parameter>=<value>[&<parameter>=<value>...]]

Example: Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

4. Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

5. Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>]
[&<parameter>…]

Where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>

where <parameter pair> is

<parameter>=<value>\r\n
[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

Request:

http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

6. Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign <*value*> to the parameter <*group*>_<*name*>.
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be

		placed at the end of the parameter list

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<parameter pair>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

7. Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than 'n' characters. The characters ",', <,>,& are invalid.
string[n~m]	Text strings longer than `n' characters and shorter than `m' characters. The characters ",', <,>,& are invalid.
password[<n>]	The same as string but displays '*' instead.
integer	Any number between (-2^{31} – 1) and (2^{31} – 1).
positive integer	Any number between 0 and (2^{32} – 1).
<m> ~ <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).

mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

7.1 system

Group: **system**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
hostname	string[64]	SD8333-E	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	0	6/6	Turn on (0) or turn off (1) all led indicators.
date	<YYYY/MM/DD>, keep, auto	<current date>	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	<current time>	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhh	<blank>	6/6	Another current time format of the

	mmYYYY.ss >			system.
ntp	<domain name>, <ip address>, <blank>	<blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -180: GMT-04:30 Caracas -160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS. 0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

				40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia

				480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	0	6/6	Enable automatic daylight saving time in time zone.
daylight_dstactualmode	1~4	1	6/7	Check current status of is daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight saving start time.
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight saving end time.
daylight_timezones	string	,-360,-320, -280,-240, -241,-200, -201,-160, -140,-120, -80,-40,0, 40,41,80, 81,82,83, 120,140, 380,400,48 0	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	0	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	N/A	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	N/A	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	0~	N/A	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the

				system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	0~	N/A	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptlang	0~	N/A	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

7.1.1 system.info

Subgroup of **system_ info** (The fields in this group are unchangeable.)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	SD8333-E	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	SD8333-E	0/7	ODM specific model name of server (eg. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"
serialnumber	<mac address>	<product mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	<product dependent >	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	9	0/7	Number of webpage languages

				available on the server.
language_i<0~(count-1)>	string[16]	<product dependent>	0/7	Available language lists.
customlanguage_maxcount	<integer>	1	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	<blank>	0/6	Custom language name.

7.2 status

Group: **status**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndi > 0)
do_i<0~(ndo-1)>	<boolean>	0	1/7	0 => Inactive, normal 1 => Active, triggered (capability.ndo > 0)
daynight	day, night	day	6/7	Current status of day, night.
onlinenum_rtsp	integer	0	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	0	6/7	Current number of HTTP push server connections.
eth_i0	<string>	<product dependent>	1/7	Get network information from mii-tool.
vi_i<0~(nvi-1)>	<boolean>	0	1/7	Virtual input 0 => Inactive 1 => Active (capability.nvi > 0)

7.3 digital input behavior define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	high	1/1	Indicates open circuit or closed circuit (inactive status)

7.4 digital output behavior define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	open	1/1	Indicate open circuit or closed circuit (inactive status)

7.5 security

Group: security

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	operator	1/6	Indicate which privileges and above can control digital output (capability.ndo > 0)
privilege_camctrl	view, operator, admin	view	1/6	Indicate which privileges and above can control PTZ (capability.ptzenabled > 0 or capability.eptz > 0)
user_i0_name	string[64]	root	6/7	User name of root
user_i<1~20>_name	string[64]	<blank>	6/7	User name
user_i0_pass	password[64]	<blank>	6/6	Root password
user_i<1~20>_pass	password[64]	<blank>	7/6	User password
user_i0_privilege	view, operator, admin	admin	6/7	Root privilege
user_i<1~20>_ privilege	view, operator, admin	<blank>	6/6	User privilege

7.6 network

Group: **network**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	<blank>	6/6	An 32-bit integer, each bit can be set separately as follows: Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service; To stop service before changing its port settings. It's **recommended** to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail. Stopped service will auto-start after changing port settings. Ex: Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480. Then, set preprocess=9 to stop both service first. "/cgi-bin/admin/setparam.cgi? network_preprocess=9&network_http_port=5556& network_rtp_videoport=20480"
type	lan, pppoe <product dependent>	lan	6/6	Network connection type.
resetip	<boolean>	1	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	<product dependent>	6/6	IP address of server.
subnet	<ip address>	<blank>	6/6	Subnet mask.
router	<ip address>	<blank>	6/6	Default gateway.

dns1	<ip address>	<blank>	6/6	Primary DNS server.
dns2	<ip address>	<blank>	6/6	Secondary DNS server.
wins1	<ip address>	<blank>	6/6	Primary WINS server.
wins2	<ip address>	<blank>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability.protocol.ieee8021x > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	eap-peap	6/6	Selected EAP method
identity_peap	String[64]	<blank>	6/6	PEAP identity
identity_tls	String[64]	<blank>	6/6	TLS identity
password	String[253]	<blank>	6/6	Password for TLS
privatekeypassword	String[253]	<blank>	6/6	Password for PEAP
ca_exist	<boolean>	0	6/6	CA installed flag
ca_time	String[20]	0	6/7	CA installed time. Represented in EPOCH
ca_size	String[20]	0	6/7	CA file size (in bytes)
certificate_exist	<boolean>	0	6/6	Certificate installed flag (for TLS)
certificate_time	String[20]	0	6/7	Certificate installed time. Represented in EPOCH
certificate_size	String[20]	0	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	0	6/6	Private key installed flag (for TLS)
privatekey_time	String[20]	0	6/7	Private key installed time. Represented in EPOCH
privatekey_size	String[20]	0	6/7	Private key file size (in bytes)

7.6.2 QOS

Subgroup of **network: qos_cos** (capability.protocol.qos.cos > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable CoS (IEEE 802.1p)
vlanid	1~4095	1	6/6	VLAN ID
video	0~7	0	6/6	Video channel for CoS
audio	0~7	0	6/6	Audio channel for CoS (capability.naudio > 0)
eventalarm	0~7	0	6/6	Event/alarm channel for CoS
management	0~7	0	6/6	Management channel for CoS
eventtunnel	0~7	0	6/6	Event/Control channel for CoS

Subgroup of **network: qos_dscp** (capability.protocol.qos.dscp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable/disable DSCP
video	0~63	0	6/6	Video channel for DSCP
audio	0~63	0	6/6	Audio channel for DSCP (capability.naudio > 0)
eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
management	0~63	0	6/6	Management channel for DSCP
eventtunnel	0~63	0	6/6	Event/Control channel for DSCP

7.6.3 IPV6

Subgroup of **network**: **ipv6** (capability.protocol.ipv6 > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable IPv6.
addonipaddress	<ip address>	<blank>	6/6	IPv6 IP address.
addonprefixlen	0~128	64	6/6	IPv6 prefix length.
addonrouter	<ip address>	<blank>	6/6	IPv6 router address.
addondns	<ip address>	<blank>	6/6	IPv6 DNS address.
allowoptional	<boolean>	0	6/6	Allow manually setup of IP address setting.

7.6.4 FTP

Subgroup of **network**: **ftp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	21, 1025~65535	21	6/6	Local ftp server port.

7.6.5 HTTP

Subgroup of **network**: **http**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	1/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
s0_accessname	string[32]	video.mjpg	1/6	HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0)
s1_accessname	string[32]	video2.mjpg	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)
s2_accessname	string[32]	video3.mjpg	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 2)
s3_accessname	string[32]	video4.mjpg	1/6	Http server push access name for stream 4 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 3)
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.

7.6.6 HTTPS port

Subgroup of **network**: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	443	1/6	HTTPS port.

7.6.7 RTSP

Subgroup of **network**: **rtsp** (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	554	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	0	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	disable	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	string[32]	live.sdp	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and capability.nmediastream > 0)
s1_accessname	string[32]	live2.sdp	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and capability.nmediastream > 1)
s2_accessname	string[32]	live3.sdp	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and capability.nmediastream > 2)
s3_accessname	string[32]	live4.sdp	1/6	RTSP access name for stream4 (capability.protocol.rtsp=1 and capability.nmediastream > 3)
s0_audiotrack	<boolean>	-1	6/6	Enable audio for stream1.
s1_audiotrack	<boolean>	-1	6/6	Enable audio for stream2.
s2_audiotrack	<boolean>	-1	6/6	Enable audio for stream3.
s3_audiotrack	<boolean>	-1	6/6	Enable audio for stream4.

7.6.7.1 RTSP multicast

Subgroup of **network_rtsp_s<0~(n-1)>_multicast,** n is stream count (capability.protocol.rtp.multicast > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	0	4/4	Enable always multicast.
ipaddress	<ip address>	For n=0, 239.128.1.99 For n=1, 239.128.1.100, and so on.	4/4	Multicast IP address.
videoport	1025 ~ 65535	5560+n*2	4/4	Multicast video port.
audioport	1025 ~ 65535	5562+n*2	4/4	Multicast audio port. (capability.naudio > 0)
metadataport	1025 ~ 65535	6560+n*2	4/4	Multicast meta data port
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

7.6.8 SIP port

Subgroup of **network**: **sip** (capability.protocol.sip> 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	5060	1/6	SIP port.

7.6.9 RTP port

Subgroup of **network**: **rtp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	5556	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)
metadataport	1025 ~ 65535	6556	6/6	Meta data channel port for RTP. (capability.protocol.rtp_unicast=1)

7.6.10 PPPoE

Subgroup of **network**: **pppoe** (capability.protocol.pppoe > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
user	string[128]	<blank>	6/6	PPPoE account user name.
pass	password[64]	<blank>	6/6	PPPoE account password.

7.7 IP Filter

Group: ipfilter

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean>	0	6/6	Enable administrator IP address.
admin_ip	String[43]	<blank>	6/6	Administrator IP address.
maxconnection	1~10	10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 1	1	6/6	Ipfilter policy : 0 => allow 1 => deny
ipv4list_i<0~9>	Single address: <ip address> Network address: <ip address / network mask> Range address:<start ip address - end ip address>	<blank>	6/6	IPv4 address list.
ipv6list_i<0~9>	String[43]	<blank>	6/6	IPv6 address list.

7.8 Video input

Group: **videoin**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mode	1	1	1/4	Set video mode.
cmosfreq	50, 60	60	4/4	CMOS frequency. (capability.videoin.type=2)
color	0, 1	1	4/4	0 =>monochrome 1 => color
flip	<boolean>	0	4/4	Flip the image.
mirror	<boolean>	0	4/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[64]	<blank>	1/4	Enclose caption.
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp on video.
enableblc	0~1	0	4/4	Enable backlight compensation (exposurecontrol => auto with IRCut)
agc	1~12 (6db~28db)	5	4/4	Set auto gain control to normal level or MAX level.

7.8.1 Video input setting per channel

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	60	4/4	CMOS frequency. (capability.videoin.type=2)
whitebalance	auto, indoor, outdoor, outdoorauto, rbgain, sodium, sodiumauto, sodiumoutdooauto,widerange, manual	outdoor	4/4	**"auto"** indicates auto white balance. **"indoor"**– 3200k base mode **"outdoor"**- 5800k base mode **"outdoorauto"** - auto white balance mode specifically for outdoors. **"rbgain"**- manual set rgain/bgain **"sodium"** - sodium vapor lamps. **"Sodiumoutdooauto"**-Sodium Vapor Lamp Outdoor Auto **"Widerange"** - Auto Tracing White balance (2000K to 10000K) **"manual"** – keep current value
zoomratiodisplay	0, 1	1	4/4	0: Do not display zoom ratio 1: Display zoom ratio
tracktextdisplay	0, 1	1	4/4	0: Do not display the object tracking hint 1: Display the object tracking hint

fixvalenable	0~2	0	4/4	indicates keep current value. 0: disable, 1: enable, 2: trigger/get current value
rgain	0~100	30	4/4	Manual set rgain value of gain control setting.
bgain	0~100	30	4/4	Manual set bgain value of gain control setting.
color	0, 1	1	4/4	0 =>monochrome 1 => color
flip	<boolean>	0	4/4	Flip the image.
mirror	<boolean>	0	4/4	Mirror the image.
ptzstatus	<integer>	2	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[64]	<blank>	1/4	Enclose caption.
textonvideo_position	top, bottom	top	4/4	Position of timestamp and video title on image
textonvideo_size	15,25,30	15	4/4	Timestamp and video title font-size
imprinttimestamp	<boolean>	0	4/4	Overlay time stamp on video.
options	quality, framerate	quality	1/4	Video input option: (1) Full HD (MAX1080P 30fps) (product dependent) (2) Exceptional frame rate (720P 60fps)

enablepreview	<boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.
s<0~(m-1)>_codectype	mpeg4, mjpeg, h264	H264	1/4	Video codec type.
s<0~(m-1)>_resolution	Reference capability_videoin_resolution	s0, s1, s3 :1280x720, s2:640x360	1/4	Video resolution in pixels.
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_maxvbrbitrate	1000~40000000	40000000	4/4	Mpeg4 max vbr bitrate
s<0~(m-1)>_mpeg4_prioritypolicy	framerate, imagequality	S0: frame rate, S1: frame rate, S2: image quality, S3: image quality	4/4	The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions. "framerate" indicates frame rate first. "imagequality" indicates image quality first.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	s0: cbr, s1: cbr, s2: cbr, s3: cbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	1~5, 99, 100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_mpeg4_qvalue	2~31	7	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 99)
s<0~(m-1)>_mpeg4_qpercent	1~100	50	4/4	Manual video quality level input. (s<0~(m-1)>_mpeg4_quant = 100)
s<0~(m-1)>_mpeg4_bitrate	1000~160000	s0: 6000000,	4/4	Set bit rate in bps when

	00 <product dependent>	s1: 6000000, s2:512000, s3: 6000000		choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mpeg4_maxframe	1~60	s0 : 60 s1 : 60 s2 : 15 s3 : 60	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_maxvbrbitrate	1000~40000000	40000000	4/4	H264 max vbr bitrate
s<0~(m-1)>_h264_priority	framerate, imagequality	S0: frame rate, S1: frame rate, S2: image quality, S3: image quality	4/4	The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions. "framerate" indicates frame rate first. "imagequality" indicates image quality first.
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	s0: cbr, s1: cbr, s2: cbr, s3: cbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_quant	1~5, 99, 100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_h264_qvalue	0~51	31	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 99)
s<0~(m-1)>_h264_qpercent	1~100	50	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 100)
s<0~(m-1)>_h264_bitrate	1000~16000000	s0:6000000, s1:6000000, s2:512000,	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".

		s3:6000000		
s<0~(m-1)>_h264_maxframe	1~60	s0 : 60 s1 : 60 s2 : 15 s3 : 60	1/4	Set maximum frame rate in fps (for H264).
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_mjpeg_prioritypolicy	framerate, imagequality	S0: frame rate S1: frame rate S2: image quality S3: image quality	4/4	The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions. "framerate" indicates frame rate first. "imagequality" indicates image quality first.
s<0~(m-1)>_mjpeg_maxvbrbitrate	1000~40000000	40000000	4/4	Jpeg max vbr bitrate
s<0~(m-1)>_mjpeg_ratecontrolmode	cbr, vbr	s0:vbr, s1: vbr, s2: vbr, s3: vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mjpeg_quant	1~5, 99, 100	3	4/4	Quality of JPEG video. 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_mjpeg_qvalue	2~97	49	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 99)
s<0~(m-1)>_mjpeg_qpercent	1~100	50	4/4	Manual video quality level input. (s<0~(m-1)>_mjpeg_quant = 100)
s<0~(m-1)>_mjpeg_maxframe	1~60	s0:10, s1:10, s2:15, s3:10	1/4	Set maximum frame rate in fps (for JPEG).

s<0~(m-1)>_mjpeg_bitrate	1000~16000000	s0:14000000, s1:14000000, s2:512000, s3:14000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_forcei	1	N/A	7/6	Force I frame.
daynight	auto,schedule, day,night	auto	4/4	auto => auto daynight night => ircut filter on day => ircut filter off schedule => scheduled ircut filter
exposurecontrol	0~3	0	4/4	Select exposure mode. 0 => Auto with IRCut 1 => Shutter priority 2 => Iris priority 3 => Manual mode
exposurelevel	0~12	6	4/4	Exposure level
agc	1~12 (6db~28db) 1: 6db 2: 8db 3: 10db ... 12: 28db	5	4/4	Set auto gain control to normal level or MAX level.
enableblc	0~1	0	4/4	Enable backlight compensation (exposurecontrol => auto with IRCut)
shutterpriority	0~14	5	4/4	Exposure time (exposurecontrol(=> shutter priority)
irispriority	1~13 (F14 ~ F1.6)	13	4/4	Iris adjustment (exposurecontrol => Iris priority)
irismanual	1~13 (F14 ~ F1.6)	13	4/4	Iris adjustment (exposurecontrol => manual)
shutterspeed	0~14 (1/1 ~ 1/10000)	5	4/4	Exposure time (exposurecontrol => manual)
gain	0~15 (0db ~ 28db)	1	4/4	Gain control (exposurecontrol => manual)

defog	0, 1	0	4/4	Enable / disable defog.
wdr_mode	0~2	1	4/4	WDR enhanced. 0: off 1: manual 2: auto
wdr_ compensation	0~2	1	4/4	WDR strength 0: low 1: medium 2: high

7.8.1.1 Alternative video input profiles per channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: **videoin_c0_profile_i<0~(m-1)>** (capability. nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable/disable this profile setting
policy	day, night, schedule	night	4/4	The mode which the profile is applied to.
begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
endtime	hh:mm	06:00	4/4	End time of schedule mode.
exposurecontrol	0~3	0	4/4	Select exposure mode. 0 => Auto with IRCut 1 => Shutter priority 2 => Iris priority 3 => Manual mode
exposurelevel	0~12	6	4/4	Exposure level
agc	1~12 (6db~28db)	5	4/4	Set auto gain control to normal level or MAX level.
enableblc	0~1	0	4/4	Enable backlight compensation (exposurecontrol => auto with IRCut)
shutterpriority	0~14	5	4/4	Exposure time (exposurecontrol(=> shutter priority)
irispriority	1~13 (F14~F1.6)	13	4/4	Iris adjustment (exposurecontrol => Iris priority)

irismanual	1~13 (F14~F1.6)	13	4/4	Iris adjustment (exposurecontrol => manual)
shutterspeed	0~14 (1/1 ~ 1/10000)	5	4/4	Exposure time (exposurecontrol => manual)
gain	0~15 (0db ~ 28db)	5	4/4	Gain control (exposurecontrol => manual)
whitebalance	auto, indoor, outdoor, outdoorauto, rbgain, sodium, sodiumauto, sodiumoutdooauto,widerange, manual	outdoor	4/4	**"auto"** indicates auto white balance. **"indoor"**– 3200k base mode **"outdoor"**- 5800k base mode **"outdoorauto"** - auto white balance mode specifically for outdoors. **"rbgain"**- manual set rgain/bgain **"sodium"** - sodium vapor lamps. **"Sodiumoutdooauto"**-Sodium Vapor Lamp Outdoor Auto **"Widerange"** - Auto Tracing White balance (2000K to 10000K) **"manual"** – keep current value
fixvalenable	0~2	0	4/4	indicates keep current value. 0: disable, 1: enable, 2: trigger/get current value
rgain	0~100	30	4/4	Manual set rgain value of gain control setting.
bgain	0~100	30	4/4	Manual set bgain value of gain control setting.
defog	0, 1	0	4/4	Enable / disable defog.
wdr_mode	0~2	1	4/4	WDR enhanced. 0: off 1: manual 2: auto
wdr_ compensation	0~2	1	4/4	WDR strength

				0: low 1: medium 2: high
daynight	auto,schedule,day,night	auto	4/4	auto => auto daynight night => ircut filter on day => ircut filter off schedule => scheduled ircut filter

7.10 IR cut control

Group: **ircutcontrol** (capability.nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
updateinterval	1~10	5	6/10	Update IR cut status interval
daymodebegintime	00:00~23:59	07:00	6/6	Day mode begin time
daymodeendtime	00:00~23:59	18:00	6/6	Day mod end time
sensitivity	0~28	8	6/6	Sensitivity of IR cut filter

7.10.1 Alternative IR cut control profiles

Group: **ircutcontrol _profile**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
profilestatus	<boolean>	0	6/6	Enable/disable this profile setting

Group: **ircutcontrol _profile_i<0~(m-1)>** (capability. nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
mode	auto, schedule, day, night	night	6/6	Active mode of this profile
daymodebegintime	00:00~23:59	07:00	6/6	Day mode begin time
daymodeendtime	00:00~23:59	18:00	6/6	Day mod end time
sensitivity	0~28	8	6/6	Sensitivity of IR cut filter

7.11 Image setting per channel

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	-5	4/4	Adjust brightness of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
dnr_mode	0,1	1	4/4	Enable/disable noise reduction
dnr_strength	1~100	100	4/4	Adjust noise reduction value of percentage
eis	0,1	0	4/4	Enable / disable electronic image stabilizer
sharpness	-3~3,100	100	4/4	Adjust sharpness of image according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of percentage when sharpness=100
saturation	-5~5,100	100	4/4	Adjust saturation of image according to mode settings.
saturationpercent	0~100	50	4/4	Adjust saturation value of percentage when saturation =100
hightvline	0,1	0	4/4	High TV line
gammacurve	0~100	0	4/4	Gamma curve
highsensitivity	0,1	1	4/4	High sensitivity
profile_i0_enable	<boolean>	0	4/4	Enable/disable this profile setting
profile_i0_policy	day, night, schedule	night	4/4	The mode which the profile is applied to.
profile_i0_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
profile_i0_endtime	hh:mm	06:00	4/4	End time of schedule mode.
profile_i0_brightness	-5~5	-5	4/4	Adjust brightness of image according to mode settings.
profile_i0_contrast	-5 ~ 5	0	4/4	Adjust contrast of image

				according to mode settings.
profile_i0_dnr_mode	0,1	1	4/4	Enable/disable noise reduction
profile_i0_dnr_strength	1~100	50	4/4	Adjust noise reduction value of percentage
profile_i0_eis	0,1	0	4/4	Enable / disable electronic image stabilizer
profile_i0_sharpness	-3~3,100	100	4/4	Adjust sharpness of image according to mode settings.
profile_i0_sharpnesspercent	0~100	50	4/4	Adjust sharpness value of percentage when sharpness=100
profile_i0_saturation	-5~5,100	100	4/4	Adjust saturation of image according to mode settings.
profile_i0_saturationpercent	0~100	50	4/4	Adjust saturation value of percentage when saturation =100
profile_i0_hightvline	0,1	0	4/4	High TV line
profile_i0_gammacurve	0~100	0	4/4	Gamma curve

7.12 Image setting for preview

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
brightness	-5~5	-5	4/4	Adjust brightness of image according to mode settings.
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according to mode settings.
dnr_mode	0,1	1	4/4	Enable/Disable noise reduction
dnr_strength	1~100	100	4/4	Adjust noise reduction value of percentage
eis	0,1	0	4/4	Enable / disable electronic image stabilizer
sharpness	-3~3,100	0	4/4	Adjust sharpness of image according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of percentage when sharpness=100

saturation	-5~5,100	100	4/4	Adjust saturation of image according to mode settings.
saturationpercent	0~100	50	4/4	Adjust saturation value of percentage when saturation =100
gammacurve	0~100	0	4/4	Gamma curve
hightvline	0,1	0	4/4	High TV line
highsensitivity	0,1	1	4/4	High sensitivity

Group: imagepreview

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
videoin_whitebalance	auto, manual, rbgain	auto	4/4	Preview of adjusting white balance of image according to mode settings
videoin_fixvalenable	0~2	0	4/4	indicates keep current value. 0: disable, 1: enable, 2: trigger/get current value
videoin_restoreatwb	1~	0	4/4	Restore of adjusting white balance of image according to mode settings
videoin_rgain	0~100	0	4/4	Manual set rgain value of gain control setting.
videoin_bgain	0~100	0	4/4	Manual set bgain value of gain control setting.

7.13 Audio detection settings

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alarm_enable	0, 1	0	4/4	Enable audio detection
alarm_level	1~100	50	4/4	Audio detection alarm level
profile_i0_enable	<boolean>	0	4/4	Enable/disable this profile setting
profile_i0_policy	day, night, schedule	night	4/4	The mode which the profile is applied to.
profile_i0_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
profile_i0_endtime	hh:mm	06:00	4/4	End time of schedule mode.
profile_i0_alarm_level	1~100	50	4/4	Audio detection alarm level

7.14 Audio input per channel

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
source	linein	linein	4/4	micin => use built-in microphone input. linein => use external microphone input.
mute	0, 1	1	1/4	Enable audio mute.
gain	1~100	65	4/4	Gain of input. (audioin_c<0~(n-1)>_source = linein)
s<0~(m-1)>_codectype	aac4 , g711, g726	g711	4/4	Set audio codec type for input.
s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	16000	4/4	Set AAC4 bitrate in bps.
s<0~(m-1)>_g711_mode	pcmu, pcma	pcmu	4/4	Set G.711 mode.
s<0~(m-1)>_g726_bitrate	16000, 24000, 32000, 40000	32000	4/4	Set G.726 bitrate in bps.
s<0~(m-1)>_g726 _bitstreampackingmode	little, big	little	4/4	Set G.726 bit streaming packing mode
s<0~(m-1)>_g726 _vlcmode	0, 1	0	4/4	Enable vlcmode for G.726

7.15 Time Shift settings

Group: **timeshift**, c for n channel products, m is stream number (capability.timeshift > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	s0:1 s1, s2,s3 : 0	4/4	Enable time shift streaming for specific stream.

7.16 Motion detection settings

Group: **motion_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[40]	<blank>	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

Group: **motion_c<0~(n-1)> profile** for m profile and n channel product (capability.nmotionprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
i<0~(m-1)>_enable	<boolean>	0	4/4	Enable profile 1 ~ (m-1).
i<0~(m-1)>_policy	day, night, schedule	night	4/4	The mode which the profile is applied to.
i<0~(m-1)>_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
i<0~(m-1)>_endtime	hh:mm	06:00	4/4	End time of schedule mode.

i<0~(m-1)>_win_i<0~2>_enable	<boolean>	0	4/4	Enable motion window.
i<0~(m-1)>_win_i<0~2>_name	string[14]	<blank>	4/4	Name of motion window.
i<0~(m-1)>_win_i<0~2>_left	0 ~ 320	0	4/4	Left coordinate of window position.
i<0~(m-1)>_win_i<0~2>_top	0 ~ 240	0	4/4	Top coordinate of window position.
i<0~(m-1)>_win_i<0~2>_width	0 ~ 320	0	4/4	Width of motion detection window.
i<0~(m-1)>_win_i<0~2>_height	0 ~ 240	0	4/4	Height of motion detection window.
i<0~(m-1)>_win_i<0~2>_objsize	0 ~ 100	0	4/4	Percent of motion detection window.
i<0~(m-1)>_win_i<0~2>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection window.

7.17 Tempering detection settings

Group: **tampering_c<0~(n-1)>** for n channel product (capability.tampering > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	32	1/7	Threshold of tamper detection.
duration	10 ~ 600	10	4/4	If tampering value exceeds the 'threshold' for more than 'duration' second(s), then tamper detection is triggered.

7.18 DDNS

Group: **ddns** (capability.ddns > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the dynamic DNS.
provider	CustomSafe100, DyndnsCustom, DyndnsDynamic, Safe100,	DyndnsDynamic	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) DynInterfree =>dyn-interfree.it CustomSafe100 => Custom server using safe100 method PeanutHull => PeanutHull IODATA => iodata.jp DO JP => ddo.jp MYDNS JP => mydns.jp Customizeddyndns => Custom server using dyndns method DP21 => dp-21.net NetHome => NetHome Co.,Ltd ADAMA_LAND => non-functional service provider Address.net => non-functional service provider Luna_VC => cybergate ddns Mars_VC => cybergate ddns Planex_VC => cybergate ddns Sun_VC => cybergate ddns Nexus_Control => nexus control DO_JP_FREE => dp-21.net (free) Epolice => epolice.com.tw PCCW => pccw.com MegaChips => megachips.co.jp Dlink =>D-LINK DlinkCN => D-LINK CN Logitec => logitec.co.jp GE_Security =>GE Security HUAGAI => huagai.com

				3322 => 3322.net ALARM => alarm.com ChangeIP => TOSHIBA NOIP => TOSHIBA SWISSCOM =>swiss.com CustomizedTZO => Customized server using TZO method <product dependent>
<provider>_hostname	string[128]	<blank>	6/6	Your DDNS hostname.
<provider>_usernameemail	string[64]	<blank>	6/6	Your user name or email to login to the DDNS service provider
<provider>_passwordkey	string[64]	<blank>	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	<blank>	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

7.19 Express link

Group: expresslink

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable express link.
state	onlycheck, onlyoffline, checkonline, badnetwork	NULL	6/6	Camera will check the status of network environment and express link URL
url	string[63]	NULL	6/6	The url user define to link to camera

7.20 UPnP presentation

Group: upnppresentation

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	1	6/6	Enable or disable the UPnP presentation service.

7.21 UPnP port forwarding

Group: upnpportforwarding

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Enable or disable the UPnP port forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UPnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

7.22 System log

Group: **syslog**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	0	6/6	Enable remote log.
serverip	<IP address>	<blank>	6/6	Log server IP address.
serverport	514, 1025~65535	514	6/6	Server port used for log.
level	0~7	6	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT 3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG
setparamlevel	0~2	0	6/6	Show log of parameter setting. 0: disable 1: Show log of parameter setting set from external. 2. Show log of parameter setting set from external and internal.

7.23 camera PTZ control

Group: **camctrl_c<0~(n-1)>** for n channel product (capability.ptzenabled)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
ccdtype	string[16]	6e	6/7	6e : SD8333
motortype	string[16]	02	6/7	02: Paugu
cameraid	1 ~ 255	1	1/4	Camera ID controlling external PTZ camera. Note: Please set your speed dome to the appropriate baud rate, and Camera ID, e.g. 2400bps, camera ID 1,2,3,,,,etc. All Camera IDs on the same controlling system (NVR or rs485 keyboard) have to be distinct. Therefore, once you send a controlling signal, each camera will only accept the inputs with the corresponding ID.
panspeed	-5 ~ 5	0	1/4	Pan speed
tiltspeed	-5 ~ 5	0	1/4	Tilt speed
zoomspeed	-5 ~ 5	0	1/4	Zoom speed
autospeed	-5 ~ 5	0	1/4	Auto pan speed
focusspeed	-5 ~ 5	0	1/4	Auto focus speed
preset_i<0~(npreset-1)>_name	string[40]	<blank>	1/4	Name of the preset location.
preset_i<0~(npreset-1)>_pan	0 ~ 7999	<blank>	1/4	Pan position at each preset location.
preset_i<0~(npreset-1)>_tilt	0 ~ 2445	<blank>	1/4	Tilt position at each preset location.
preset_i<0~(npreset-1)>_zoom	0 ~ 16384	<blank>	1/4	Zoom position at each preset location.
preset_i<0~(npreset-1)>_focus	4096 ~ 53248	<blank>	1/4	Focus position at each preset location.
preset_i<0~(npreset-1)>_fliped	0,1	<blank>	1/4	Flip side at each preset location.
patrol_i<0~39>_name	string[40]	<blank>	1/4	(For internal device) The name of patrol location

patrol_i<0~39>_ dwelling	0 ~ 999	<blank>	1/4	(For internal device) The dwelling time of each patrol location
disablemdonptz	<boolean>	1	1/4	Disable motion detection on PTZ operation.
defaulthome	<boolean>	1	1/4	This field tells system to use default home position or not.
axisx	0 ~ 7999	0	1/4	Custom home pan position.
axisy	0 ~ 2445	0	1/4	Custom home tilt position.
axisz	0 ~ 16384	0	1/4	Custom home zoom position.
axisf	4096 ~ 49152	4096	1/4	Custom home focus position.
axisflip	0,1	0	1/4	Custom home flip side.
returnhome	0,1	0	1/4	Enable/disable return home while idle.
returnhomeinterval	1~999	5	1/4	While idle over this time interval, idle action will be taken.
digitalzoom	<boolean>	0	1/4	Enable/disable digital zoom
idleaction_enable	0~1	1	1/4	Enable/disable idle action while idle
idleaction_type	pan,patrol,hom e,objtrack,prev	prev	1/4	This field tells what kind of action should be taken while idle.
idleaction_interval	1~999	5	1/4	While idle over this time interval, idle action will be taken.
horizontalalignment	<boolean>	0	1/4	Once you enable this feature, a reference line will be visible when the camera tilt is under 0° or over 180° to help verify that the camera is mounted to a flat surface.
osdzoom	<boolean>	0	1/4	Show zoom ratio text on video.
zoomenhance	<boolean>	0	1/4	Enable / Disable zoom enhancement
tour_index	-1, 0~19	0	1/4	Index of the enabled tour group, from 0 to 19. Set -1 to disable all the tour groups.
tour_i<0~(m-1)>_na me	string[40]	<blank>	1/4	Name of the tour.
tour_i<0~(m-1)>_typ e	<boolean>	<blank>	1/4	0 = Recorded tour 1 = Preset tour
tour_i<0~(m-1)>_sp eed	-5 ~ 5	<blank>	1/4	Preset tour: pan and tilt speed when moving between presets.

				Recorded tour: unnecessary.
tour_i<0~(m-1)>_checklist	string[512]	<blank>	1/4	The indexes of preset positions, separated by ","
tour_i<0~(m-1)>_dwelltime	string[512]	<blank>	1/4	Preset tour: time to wait before moving to the next preset position, separated by "," Recorded tour: number of seconds to wait before continuing a loop tour.

7.24 UART control

Group: **uart_i<0~(n-1)>** n is uart port count (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
cameraid	1~255	1	4/4	Camera ID controlling external PTZ camera. Note: Please set your speed dome to the appropriate baud rate, and Camera ID, e.g. 2400bps, camera ID 1,2,3,,,,etc. All Camera IDs on the same controlling system (NVR or rs485 keyboard) have to be distinct. Therefore, once you send a controlling signal, each camera will only accept the inputs with the corresponding ID.
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	2400	4/4	Set baud rate of COM port.
databit	5,6,7,8	8	4/4	Data bits in a character frame.
paritybit	none, odd, even	none	4/4	For error checking.

stopbit	1,2	1	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	rs485	4/4	RS485 or RS232.

7.25 SNMP

Group: **snmp** (capability.snmp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
v2	0~1	0	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	0	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	Private	6/6	Read/write security name
secnamero	string[31]	Public	6/6	Read only security name
authpwrw	string[8~128]	<blank>	6/6	Read/write authentication password
authpwro	string[8~128]	<blank>	6/6	Read only authentication password
authtyperw	MD5,SHA	MD5	6/6	Read/write authentication type
authtypero	MD5,SHA	MD5	6/6	Read only authentication type
encryptpwrw	string[8~128]	<blank>	6/6	Read/write passwrd
encryptpwro	string[8~128]	<blank>	6/6	Read only password
encrypttyperw	DES	DES	6/6	Read/write encryption type
encrypttypero	DES	DES	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Read only community
syslocation	0~128	<blank>	6/6	System location
syscontact	0~128	<blank>	6/6	System contact

7.26 Layout configuration

Group: **layout** (New version)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1	1/6	0 => Custom logo 1 => Default logo
logo_link	string[128]	http://www.vivotek.com	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	0	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
custombutton_manualtrigger_show	<boolean>	1	1/6	Show or hide manual trigger (VI) button in homepage 0 -> Hidden 1 -> Visible
theme_option	1~4	1	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	#000000	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackground	string[7]	#c4eaff	1/6	Background color of control area.
theme_color_configbackground	string[7]	#0186D1	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	#c4eaff	1/6	Background color of video area.
theme_color_case	string[7]	#0186D1	1/6	Frame color

7.27 Privacy mask

Group: **privacymask3d_c<0~(n-1)>** for n channel product

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	4/4	Enable the 3D privacy mask
color	0~14	0	4/4	Privacy mask color
win_i<0~23>_name	string[40]	<blank>	4/4	Name of the privacy mask window.
win_i<0~23>_pan	0 ~ 7999	0	4/4	Pan position of window position.
win_i<0~23>_tilt	0 ~ 2445	0	4/4	Tilt position of window position.
win_i<0~23>_zoom	0 ~ 16384	0	4/4	Zoom position of window position.
win_i<0~23>_fliped	0,1	0	4/4	Flip side of window position.
win_i<0~23>_width	0 ~ 80	0	4/4	Width of privacy mask window.
win_i<0~23>_height	0 ~ 60	0	4/4	Height of privacy mask window.

7.28 Capability

Group: capability

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	<string>	0300a	0/7	The HTTP API version.
bootuptime	<positive integer>	150	0/7	Server bootup time.
nir	0, <positive integer>	0	0/7	Number of IR interfaces. (Recommand to use ir for built-in IR and extir for external IR)
npir	0, <positive integer>	0	0/7	Number of PIRs.
ndi	0, <positive integer>	4	0/7	Number of digital inputs.
nvi	0,	3	0/7	Number of virtual inputs

	<positive integer>			(manual trigger)
ndo	0, <positive integer>	2	0/7	Number of digital outputs.
naudioin	0, <positive integer>	1	0/7	Number of audio inputs.
naudioout	0, <positive integer>	1	0/7	Number of audio outputs.
nvideoin	<positive integer>	1	0/7	Number of video inputs.
nmediastream	<positive integer>	4	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	2	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	1	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0	0/7	Number of UART interfaces.
nvideoinprofile	<positive integer>	1	0/7	Number of video input profiles.
nmotionprofile	0, <positive integer>	1	0/7	Number of motion profiles.
nmotion	0, <positive integer>	3	0/7	Number of motion window.
ptzenabled	0, <positive integer>	63	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in) Bit 2 => Support pan operation, 0(not support), 1(support)

				Bit 3 => Support tilt operation; 0(not support), 1(support) Bit 4 => Support zoom operation; 0(not support), 1(support) Bit 5 => Support focus operation; 0(not support), 1(support) Bit 6 => Support iris operation; 0(not support), 1(support) Bit 7 => External or built-in PT; 0(built-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
windowless	<boolean>	1	0/7	Indicate whether to support windowless plug-in.
evctrlchannel	<boolean>	1	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	1	0/7	Indicate whether to support joystick control.
ptz_panspeedlv	<positive integer>	127	0/7	The maximum speed level of pan moving.
ptz_tiltspeedlv	<positive integer>	127	0/7	The maximum speed level of tilt moving.
ptz_zoomspeedlv	<positive integer>	7	0/7	The maximum speed level of zoom moving

ptz_focusspeedlv	0, <positive integer>	7	0/7	The maximum speed level of focus moving. 3.2-1
ptz_minpan	<positive integer>	0	0/7	The lower limit for pan position. 3.2-1
ptz_maxpan	<positive integer>	7999	0/7	The upper limit for pan position. 3.2-1
ptz_minpanangle	< integer>	0	0/7	The lower limit for pan angle. 3.2-1
ptz_maxpanangle	< integer>	360	0/7	The upper limit for pan position. 3.2-1
ptz_mintilt	<positive integer>	0	0/7	The lower limit for tilt position. 3.2-1
ptz_maxtilt	<positive integer>	2445	0/7	The upper limit for tilt position. 3.2-1
ptz_mintiltangle	< integer>	-20	0/7	The lower limit for tilt angle. 3.2-1
ptz_maxtiltangle	< integer>	90	0/7	The upper limit for tilt angle. 3.2-1
ptz_minzoom	0, <positive integer>	0	0/7	The lower limit for zoom position. 3.2-1
ptz_maxzoom	0, <positive integer>	16384	0/7	The upper limit for zoom position. 3.2-1
ptz_maxdzoom	0, <Positive Integer>	31424	0/7	The upper limit for zoom position. 3.2-1
ptz_minfocus	0, <positive integer>	4096	0/7	The lower limit for focus position. 3.2-1
ptz_maxfocus	0, <positive integer>	53248	0/7	The upper limit for focus position. 3.2-1
storage_dbenabled	<boolean>	1	0/7	Media files are indexed in database.
protocol_https	< boolean >	1	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	1	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	1	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	10	0/7	The maximum allowed simultaneous connections.
protocol_maxgenconnection	<positive	10	0/7	The maximum general

	integer>			streaming connections .
protocol_maxmegaconnection	<positive integer>	0	0/7	The maximum megapixel streaming connections.
protocol_rtp_multicast_ scalable	<boolean>	1	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_ backchannel	<boolean>	1	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	1	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	1	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	1	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	1	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	1	0/7	Indicate whether to support IPv6.
protocol_pppoe	<boolean>	1	0/7	Indicate whether to support PPPoE.
protocol_ieee8021x	<boolean>	1	0/7	Indicate whether to support IEEE802.1x.
protocol_qos_cos	<boolean>	1	0/7	Indicate whether to support CoS.
protocol_qos_dscp	<boolean>	1	0/7	Indicate whether to support QoS/DSCP.
protocol_ddns	<boolean>	1	0/7	Indicate whether to support DDNS.
videoin_type	0, 1, 2	2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	176x144,384x216, 640x360,1280x720	0/7	Available resolutions list.
videoin_maxframerate	<a list of	60,60,60,60	0/7	Available maximum frame

	available maximum frame rate separated by commas>			list.
videoin_codec	mpeg4, mjpeg, h264	mpeg4, mjpeg, h264	0/7	Available codec list.
videoin_streamcodec	7,7,7,7	A list of <Positive Integer>	0/7	This equals "capability_videoin_c0_streamcodec". * This is kept for compatibility.
videoin_c<n>_streamcodec	7,7,7,7	A list of <Positive Integer>	0/7	Represent supported codec types of each stream. This contains a list of positive integers, split by comma. Each one stands for a stream, and the definition is as following: Bit 0: Support MPEG4. Bit 1: Support MJPEG Bit 2: Support H.264 Ex: IP8371E has 1 channel 4 streams, all streams support MPEG4, MJPEG, and H.264, then this will be "7,7,7,7". Ex: IP7161 has 1 channel 4 streams, all streams support MPEG4, and MJPEG, then this will be "3,3,3,3". * The number of integers is equal to "capability_nmediastream

				". * Only available when [httpversion] >= 0300
videoin_flexiblebitrate	1	0, 1	0/7	1: Support flexible bit rate control 0: Non-support flexible bit rate control. * More detail, see 5.5 Codec: H264, 5.6 Codec: MPEG4, 5.7 Codec: MJPEG * Only available when [httpversion] >= 0300
timeshift	<boolean>	1	0/7	Indicate whether to support time shift caching stream.
audio_aec	<boolean>	0	0/7	Indicate whether to support acoustic echo cancellation.
audio_mic	<boolean>	0	0/7	Indicate whether to support built-in microphone input.
audio_extmic	<boolean>	1	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	1	0/7	Indicate whether to support external line input. (It will be replaced by audio_mic and audio_extmic.)
audio_lineout	<boolean>	1	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0	0/7	Indicate whether to support headphone output.
audioin_codec	aac4, g711, g726	aac4, g711, g726	0/7	Available codec list for audio input.

audioout_codec	g711	g711	0/7	Available codec list for SIP.
camctrl_httptunnel	<boolean>	0	0/7	Indicate whether to support httptunnel.
camctrl_privilege	<boolean>	1	0/7	Indicate whether to support "Manage Privilege" of PTZ control in the Security page. 1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi 0: support only /cgi-bin/viewer/camctrl.cgi
uart_httptunnel	<boolean>	0	0/7	Indicate whether to support HTTP tunnel for UART transfer.
transmission_mode	Tx, Rx, Both	Tx	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	1	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0	0/7	Indicate whether to support wireless.
wireless_s802dot11b	<boolean>	0	0/7	Indicate whether to support wireless 802.11b+.
wireless_s802dot11g	<boolean>	0	0/7	Indicate whether to support wireless 802.11g.
wireless_s802dot11g	<boolean>	0	0/7	Indicate whether to support wireless 802.11n.
wireless_beginchannel	1 ~ 14	N/A	0/7	Indicate the begin channel of wireless network
wireless_endchannel	1 ~ 14	N/A	0/7	Indicate the end channel of wireless network
wireless_encrypt_wep	<boolean>	0	0/7	Indicate whether to support wireless WEP.

wireless_encrypt_wpa	<boolean>	0	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0	0/7	Indicate whether to support wireless WPA2.
derivative_brand	<boolean>	1	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
npreset	0, <positive integer>	256	0/7	Number of preset locations
eptz	0, <positive integer>	0	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not. Bit 1 => stream 2 supports ePTZ or not. The rest may be deduced by analogy
nanystream	0, <positive integer>	0	0/7	number of any media stream per channel
iva	<boolean>	0	0/7	Indicate whether to support Intelligent Video analysis
ir	<boolean>	0	0/7	Indicate whether to support built-in IR led.
extir	<boolean>	1	0/7	Indicate whether to support external IR led.
whitelight	<boolean>	0	0/7	Indicate whether to support white light led.
iris	<boolean>	1	0/7	Indicate whether to support iris control.
tampering	<boolean>	0	0/7	Indicate whether to support tampering detection.

temperature	<boolean>	0	0/7	Indicate whether to support temperature detection.
test_ac	<boolean>	1	0/7	Indicate whether to support test ac key.
version_onvifdaemon	<string>	1.8.0.9	0/7	Indicate ONVIF daemon version
version_onvifevent	<string>	1.3.0.7	0/7	Indicate ONVIF event version
version_genetec	<string>	1.0.2.6	0/7	Indicate Genetec version
media_totalspace	<positive integer>	20000	0/7	Available memory space (KB) for media.
media_snapshot_sizepersecond	<positive integer>	500	0/7	Maximum size (KB) of one snapshot image.
media_snapshot_maxpreevent	<positive integer>	7	0/7	Maximum snapshot number before event occurred.
media_snapshot_maxpostevent	<positive integer>	7	0/7	Maximum snapshot number after event occurred.
media_videoclip_maxsize	<positive integer>	8192	0/7	Maximum size (KB) of a videoclip.
media_videoclip_maxlength	<positive integer>	20	0/7	Maximum length (second) of a videoclip.
media_videoclip_maxpreevent	<positive integer>	9	0/7	Maximum duration (second) after event occurred in a videoclip.
localstorage_manageable	<boolean>	1	0/7	Indicate whether manageable local storage is supported.
localstorage_seamless	<boolean>	1	0/7	Indicate whether seamless recording is supported.
localstorage_modnum	0, <positive integer>	4	0/7	The maximum MOD connection numbers.
localstorage_modversion	<string>	1.0.2.5	0/7	Indicate MOD daemon version.
localstorage_slconnum	<positive integer>	1	0/7	Seamless connection number.

supportsd	<boolean>	1	0/7	Indicate whether to support local storage.
remotecamctrl_master	0, <positive integer>	0	0/7	Indicate whether to support remote auxiliary camera (master side), this value means supporting max number of auxiliary camera.
remotecamctrl_slave	<boolean>	1	0/7	Indicate whether to support remote camera control (slave side).
adaptiverecording	<boolean>	1	0/7	Indicate whether to support adaptive recording.
adaptivestreaming	<boolean>	1	0/7	Indicate whether to support adaptive streaming.
vadp	<positive integer>	251	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => VADP interface Bit 1 => Capture video raw data Bit 2 => Support encode jpeg Bit 3 => Capture audio raw data Bit 4 => Support event trigger Bit 5 => Support license registration Bit 6 => Support shared memory API
privacymask_axistype	0,1,2	2	0/7	Describes the technical method in which to implement a privacy mask. 0 (Unidentified. The firmware is in an earlier version)

				1 (The privacy mask is a 2D version) 2 (The privacy mask is a 3D version) A 3D privacy mask denotes that the camera maintains mask position and size while PTZ is in motion. In the 2D version, each mask is maintained in the viewing window with a fixed size, regardless of the motors driving PTZ.

Group: capability_videoin_c<n>,
n denotes the channel index, with a range from 0 to one less than the value of “capability_nvideoin".

* Only available when the value of [httpversion] is greater than or equal to 0300

NAME	VALUE	Default	SECURITY (get/set)	DESCRIPTION
nmode	<Positive Integer>	1	0/7	Indicate how many video modes supported by this channel.
maxsize	<WxH>	1280x720	0/7	The maximum resolution of all modes in this channel, the unit is pixel. * We call this as "**Full Scene**".
mode	<Integer>	0	0/7	Indicate current video mode.
nresolution	<Positive Integer>	4	0/7	How many resolution options (listed in "resolution") in current video mode.
resolution	A list of <WxH>	176x144,384x216,640x360,1280x720	0/7	Resolution options in current video mode. These options are the possible options for "videoin_c<n>_s<m>_resolution", see 5.1 Resolution. The last one is the maximum resolution in current mode. * The element number is defined as "nresolution" in

NAME	VALUE	Default	SECURITY (get/set)	DESCRIPTION
				this group.
maxframerate	A list of <Integer>	60,60,60,60	0/7	Indicate frame rate that the video source outputs in current video mode. One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter may be changed when "videoin_c<n>_cmosfreq"=50 or "videoin_c<n>_modulation"=pal. Ex: 30 fps is changed to 25 fps, 60 fps is changed to 50 fps, and so on.
mpeg4_maxframerate	A list of <Integer> and "-"	60,60,60,60	0/7	Maximum fps that the device can encoded one stream with MPEG4 on resolutions in current video mode. "-" means not support. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter may be changed when "videoin_c<n>_cmosfreq"=50 or "videoin_c<n>_modulation"=pal. Ex: 30 fps is changed to 25 fps, 60 fps is changed to 50 fps, and so on. More details, see 5.6 Codec: MPEG4. * Only available when 'mpeg4' is listed in "capability_videoin_codec".

NAME	VALUE	Default	SECURITY (get/set)	DESCRIPTION
mpeg4_maxbitrate	<Positive Integer>	40000000	0/7	Maximum bitrates of MPEG4. The unit is bps. * Only available when 'mpeg4' is listed in "capability_videoin_codec". * More details, see 5.6 Codec: MPEG4.
mjpeg_maxframerate	A list of <Positive Integer> and "-"	60,60,60,60	0/7	Maximum fps that the device can encoded one stream with MJPEG on resolutions in current video mode. "-" means not support. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter may be changed when "videoin_c<n>_cmosfreq"=50 or "videoin_c<n>_modulation"=pal. Ex: 30 fps is changed to 25 fps, 60 fps is changed to 50 fps, and so on. More details, see 5.7 Codec: MJPEG. * Only available when 'mjpeg' is listed in "capability_videoin_codec".
mjpeg_maxbitrate	<Positive Integer>, -	40000000	0/7	Maximum bitrates of MJPEG. The unit is bps. "-" means MJPEG does not support bit rate control. * Only available when 'mjpeg' is listed in "capability_videoin_codec". * More details, see 5.7 Codec: MJPEG.

NAME	VALUE	Default	SECURITY (get/set)	DESCRIPTION
h264_maxframerate	A list of <Positive Integer> and "-"	60,60,60,60	0/7	Maximum fps that the device can encoded one stream with H.264 on resolutions in current video mode. "-" means not support. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter may be changed when "videoin_c<n>_cmosfreq"=50 or "videoin_c<n>_modulation"=pal. Ex: 30 fps is changed to 25 fps, 60 fps is changed to 50 fps, and so on. More details, see 5.5 Codec: H264. * Only available when 'h264' is listed in "capability_videoin_codec".
h264_maxbitrate	<Positive Integer>	40000000	0/7	Maximum bitrates of H.264. The unit is bps. * Only available when 'h264' is listed in "capability_videoin_codec". * More details, see 5.5 Codec: H264.

Group: capability_videoin_c<n>_mode<m>,

n denotes the channel index, with a range from 0 to one less than the value of“capability_nvideoin”;

m denotes the stream index, with a range from 0 to one less than the value of "capability_nmediastream".

NAME	VALUE	Default	SECURITY (get/set)	DESCRIPTION
effectivepixel	<WxH>	1280x720	0/7	The visible area of full scene in this video mode. The unit is pixel in source. * This value must <= "capability_videoin_c<n>_maxsize" * If "effectivepixel"<"capability_videoin_c<n>_maxsize", then the visible area is located at the center of full scene.
outputsize	<WxH>	1280x720	0/7	The output size of source, equal to the captured size by device, in this video mode. The unit is pixel. This value is used as a basic coordinate system for many features, like ePTZ, privacy mask, motion, etc. * Source (most for image sensor) may perform scale or binning, etc on image data, and output data with smaller size. This parameter is designed to represent this.
binning	0, 1, 3	0	0/7	Indicate binning is used or not in this video mode. 0: No binning 1: 2x2 binning 3: 3x3 binning * Binning is a technology to increase light sensitivity by combining multiple pixels to one. The drawback is reduced resolution. We design this parameter to disclose this information.
nresolution	<Positive Integer>	4	0/7	How many resolution options in this video mode.
resolution	A list of <WxH>	176x144,384x216,640x360,1280x720	0/7	Resolution options in this video mode. The last one is the maximum resolution in this video mode. * The element number is defined as "nresolution" in this group.

NAME	VALUE	Default	SECURITY (get/set)	DESCRIPTION
maxframerate	A list of <Positive Integer>	60,60,60,60	0/7	Indicates frame rate that the video source outputs in this video mode. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter records the frame rate when "videoin_c<n>_cmosfreq"=60 or "videoin_c<n>_modulation"=ntsc
maxfps_mpeg4	A list of <Positive Integer> and "-"	60,60,60,60	0/7	Maximum fps which the device can encoded with MPEG4 on resolutions in this video mode. "-" means not support. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter records the frame rate when "videoin_c<n>_cmosfreq"=60 or "videoin_c<n>_modulation"=ntsc * Only available when 'mpeg4' is listed in "capability_videoin_codec".
maxfps_mjpeg	A list of <Positive Integer> and "-"	60,60,60,60	0/7	Maximum fps which the device can encoded with MJPEG on resolutions in this video mode. "-" means not support. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter records the frame rate when "videoin_c<n>_cmosfreq"=60 or "videoin_c<n>_modulation"=ntsc * Only available when 'mjpeg' is listed in "capability_videoin_codec".

NAME	VALUE	Default	SECURITY (get/set)	DESCRIPTION
maxfps_h264	A list of <Positive Integer> and "-"	60,60,60,60	0/7	Maximum fps which the device can encoded with H.264 on resolutions in this video mode. "-" means not support. * One to one mapping to the resolution in "resolution". * The element number is defined as "nresolution" in this group. * This parameter records the frame rate when "videoin_c<n>_cmosfreq"=60 or "videoin_c<n>_modulation"=ntsc * Only available when 'h264' is listed in "capability_videoin_codec".
description	<String [128]>	720P HD (16:9) (MAX 60 fps)	0/7	Description about this mode.

7.29 Customized event script

Group: event_customtaskfile_i<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Custom script identification of this entry.
date	string[4~20]	<blank>	6/6	Date of custom script.
time	string[4~20]	<blank>	6/6	Time of custom script.

7.30 Event setting

Group: **event_i**<0~2>

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
name	string[40]	<blank>	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.

priority	0, 1, 2	1	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	10	6/6	Delay in seconds before detecting the next event.
trigger	boot, di, motion, seq, recnotify, volalarm, vi vadp	boot	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "motion" = Video motion detection "seq" = Periodic condition "recnotify" = Recording notification. "volalarm" = Audio detection. "vi" = Virtual input. "vadp" = VADP trigger
triggerstatus	String[40]	trigger	6/6	The status for event trigger
exttriggerstatus	String[40]	<blank>	6/6	The status for event trigger
exttriggerstatus1	String[40]	<blank>	6/6	The status for event trigger
exttriggerstatus2	String[40]	<blank>	6/6	The status for event trigger
exttriggerstatus3	String[40]	<blank>	6/6	The status for event trigger
di	0~15	1	6/6	Indicate the source id of di trigger. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	0~7	0	6/6	Indicate the source window id of motion detection. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
mdwin0	0~7	0	6/6	Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled.
valevel	<boolean>	0	6/6	Enable/Disable audio detect.
valevel0	<boolean>	0	6/6	Enable/Disable audio detect profile.

vi	0~7	0	6/6	Indicate the source id of vi trigger. This field is required when trigger condition is "vi".
inter	1~999	1	6/6	Interval of snapshots in minutes. This field is used when trigger condition is "seq".
weekday	0~127	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	00:00	6/6	Begin time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)
action_do_i<0~(ndo-1)>_enable	0, 1	0	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	1	6/6	Duration of the digital output trigger in seconds.
action_goto_enable	<Boolean>	0	6/6	Enable/disable ptz goto preset position on event triggered.
action_goto_name	string[40]	<blank>	6/6	Specify the preset name that ptz goto on event triggered.
action_goto_sync	<Boolean>	0	6/6	Capture media after moving to the location
action_cf_enable	<Boolean>	0	6/6	Enable or disable sending media to SD card.
action_cf_folder	string[128]	<blank>	6/6	Path to store media.
action_cf_media	0~4, 101	<blank>	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	1	6/6	Enable this to create folders by date, time, and hour automatically.

action_cf_backup	<Boolean>	0	6/6	Enable or disable the function that send media to SD card for backup if network is disconnected.
action_server_i<0~4>_enable	0, 1	0	6/6	Enable or disable this server action.
action_server_i<0~4>_media	0~4, 101	<blank>	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	0	6/6	Enable this to create folders by date, time, and hour automatically.
vadp	<integer>	0	6/6	Indicate the source id of vadp event notification. Each bit corresponds to one vadp source, and the LSB indicates source id 0. For example, to detect event from any one of source id 0, 1 and 3, set vadp to 11.

7.31 Server setting for event action

Group: **server_i**<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	email, ftp, http, ns	email	6/6	Indicate the server type: “email” = email server “ftp” = FTP server “http” = HTTP server “ns” = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.
http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.

ftp_passive	0, 1	1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.
email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[640]	NULL	6/6	Email address of the recipient.
ns_location	string[128]	NULL	6/6	Location to upload or store the media.
ns_username	string[64]	NULL	6/6	Username to log in to the server.
ns_passwd	string[64]	NULL	6/6	Password of the user.
ns_workgroup	string[64]	NULL	6/6	Workgroup for network storage.

7.32 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	snapshot	6/6	Media type to send to the server or store on the server.
snapshot_source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	Snapshot<1~5>_	6/6	Indicate the prefix of the filename. media_i0=> Snapshot1_ media_i1=> Snapshot2_ media_i2=> Snapshot3_ media_i3=> Snapshot4_ media_i4=> Snapshot5_

snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
videoclip_source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	VideoClip<1~5>_	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	0	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 20	5	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 8192	1000	6/6	Maximum size of one video clip file in Kbytes.

7.33 Recording

Group: **recording_i**<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
trigger	schedule, networkfail	schedule	6/6	The event trigger type schedule: The event is triggered by schedule networkfail: The event is triggered by the failure of network connection.
enable	0, 1	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and so on.

limitsize	0,1	0	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	0	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	1	6/6	0: Disable recording notification 1: Enable recording notification
notifyserver	0~31	0	6/6	Indicate which notification server is scheduled. One bit represents one application server (server_i0~i4). bit0 (LSB) = server_i0. bit1 = server_i1. bit2 = server_i2. bit3 = server_i3. bit4 = server_i4. For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.
weekday	0~127	127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	00:00	6/6	Start time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	<blank>	6/6	Indicate the prefix of the filename.
cyclesize	200~	100	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	0~	100	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.

dest	cf, 0,1,2,3,4	cf	6/6	The destination to store the recorded data. "cf" means local storage (CF or SD card). "0" means the index of the network storage.
cffolder	string[128]	NULL	6/6	Folder name.
adaptive_enable	0,1	0	6/6	Indicate whether the adaptive recording is enabled
adaptive_preevent	0~9	1	6/6	Indicate when is the adaptive recording started before the event trigger point (seconds)
adaptive_postevent	0~10	1	6/6	Indicate when is the adaptive recording stopped after the event trigger point (seconds)
maxsize	100~2000	100	6/6	Unit: Mega bytes. When this condition is reached, recording file is truncated.
maxduration	60~3600	60	6/6	Unit: Second When this condition is reached, recording file is truncated.

7.34 HTTPS

Group: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	To enable or disable secure HTTP.
policy	<Boolean>	0	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection
method	auto, manual, install	auto	6/6	auto => Create self-signed certificate automatically. manual => Create self-signed certificate manually. install => Create certificate request and install.
status	-3 ~ 1	0	6/6	Specify the https status. -3 = Certificate not installed -2 = Invalid public key

				-1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	TW	6/6	Country name in the certificate information.
stateorprovincename	string[128]	Asia	6/6	State or province name in the certificate information.
localityname	string[128]	Asia	6/6	The locality name in the certificate information.
organizationname	string[64]	VIVOTEK.Inc	6/6	Organization name in the certificate information.
unit	string[64]	VIVOTEK.Inc	6/6	Organizational unit name in the certificate information.
commonname	string[64]	www.vivotek.com	6/6	Common name in the certificate information.
validdays	0 ~ 9999	3650	6/6	Valid period for the certification.

7.35 Storage management setting

Currently it's for local storage (SD, CF card)

Group: **disk_i<0~(n-1)>** n is the total number of storage devices. (capability.storage.dbenabled > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
cyclic_enabled	<boolean>	0	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean>	0	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	<positive integer>	7	6/6	To specify the expired days for automatic clean up.

7.36 Object tracking setting

Group: **sdobjtrack**.

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
objsize_type	-1~2	-1	1/4	Type of object size. -1 : customized width and height 0 : object size = 30 x 30 1 : object size = 10 x 20 2 : object size = 10 x 10
objsize_customized_width	10~320	30	1/4	The minimum width of tracking target.
objsize_customized_height	10~240	30	1/4	The minimum heght of tracking target.
sensitivity	0~2	1	1/4	Tracking sensitivity. 0 : Low 1 : Medium 2 : High

7.37 Seamless recording setting

Group: **seamlessrecording** (capability.localstorage.seamless > 0)

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
diskmode	seamless, manageable	seamless	1/6	“seamless” indicates enable seamless recording. “manageable” indicates disable seamless recording.
maxconnection	3	3	1/6	Maximum number of connected seamless streaming.
stream	1~4	1	1/6	(Internal used, read only)
output	0~3	2	1/6	(Internal used, read only)
enable	<boolean>	0	1/6	Indicate whether seamless recording is recording to local storage or not at present. (Read only)
guid<0~2>_id	string[127]	<blank>	1/6	The connected seamless streaming ID. (Read only)

guid<0~2>_number	0~3	0	1/6	Number of connected seamless streaming with guid<0~2>_id. (Read only)

7.38 VIVOTEK Application Development Platform setting

Group: **vadp**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
version	<string>	1.2.0.0	6/7	Indicate the VADP version.
number	string[128]	<product dependent>	6/7	This number is used to register license key for VADP application.
resource_total_memory	<integer>	<product dependent>	6/7	Indicate total available memory size for VADP modules.
resource_total_storage	<integer>	<product dependent>	6/7	Indicate total size of the internal storage space for storing VADP modules.
resource_free_memory	<integer>	32492	6/7	Indicate free memory size for VADP modules.
resource_free_storage	<integer>	19684	6/7	Indicate current free storage size for uploading VADP modules.
module_number	<integer>	0	6/7	Record the total module number that already stored in the system.
module_order	string[40]	<blank>	6/6	The execution order of the enabled modules.
module_save2sd	<boolean>	0	6/6	Indicate if the module should be saved to SD card when user want to upload it. If the value is false, save module to the internal storage space and it will occupy storage size.

Group: vadp_module_i<0~(n-1)> n = 10

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	0	6/6	Indicate if the module is enabled or not. If yes, also add the index of this module to the module_order.
name	string[40]	<blank>	6/6	Module name
url	string[120]	<blank>	6/6	Define the URL string after the IP address if the module provides it own web page.
vendor	string[40]	<blank>	6/6	The provider of the module.
vendorurl	string[120]	<blank>	6/6	URL of the vendor.
version	string[40]	<blank>	6/6	Version of the module.
license	string[40]	<blank>	6/6	Indicate the license status of the module.
path	string[40]	<blank>	6/6	Record the storage path of the module.
initscr	string[40]	<blank>	6/6	The script that will handle operation commands from the system.
status	string[40]	off	6/6	Indicate the running status of the module.
statmsg	string[128]	<blank>	6/6	Indicate the message that will be show on the running status when mouse over.
vvtklicensemec	string[40]	<blank>	6/7	Indicate the module use VIVOTEK license mechanism

Group: **vadp_event**

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
ntrigger	<integer>	<product dependent>	6/7	Indicate the number of topics to be transferred to event manager for trigger.
triggerlist_i<0~(n-1)>_topic	<string>	<blank>	6/6	Indicate the event notification with this topic will be transferred to event manager as trigger.

				n is equal to ntrigger above.

8. Useful Functions

8.1 Drive the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>]
```

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

8.2 Query Status of the Digital Input (capability.ndi > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all of the digital input statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1 .

Request:

http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

di1=1\r\n

8.3 Query Status of the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the digital output statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: <*length*>\r\n

\r\n

[do0=<state>]\r\n

[do1=<state>]\r\n

[do2=<state>]\r\n

[do3=<state>]\r\n

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1.

Request:

http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

```
\r\n
do1=1\r\n
```

8.4 3D Privacy Mask

Note: This request requires admin user privilege

<SD81X1> You can set privacy mask only at zoom 1x. To go back to zoom 1x directly, please send this cgi command: "/cgi-bin/camctrl/camposition.cgi?setzoom=0"

Method: GET/POST

Syntax:

Fixed in center :

http://<*servername*>/cgi-bin/admin/setpm3d.cgi?method=<value>&name=<value>&[maskheight=<value>&maskwidth=<value>&return=<return page>]

Drag to move :

http://<*servername*>/cgi-bin/admin/setpm3d.cgi?method=<value>&name=<value>&[maskheight=<value>&maskwidth=<value>&return=<return page>&maskcx=<value>&maskcy=<value>&videosize=1280x720]

PARAMETER	VALUE	DESCRIPTION
method	add	Add a 3D privacy mask at current location
	delete	Delete a 3D privacy mask
	edit	Edit a 3D privacy mask
maskname	string[40]	3D privacy mask name
maskheight	integer	3D privacy mask height
maskwidth	integer	3D privacy mask width
maskcx	0~1280	X offset of mask location. (for drag to move)
maskcy	0~720	Y offset of mask location. (for drag to move)
return	<return page>	Redirect to page <*return page*> after the 3D privacy mask is configured. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.5 Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	<available resolution>	0	The resolution of the image.
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	<product dependent>	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

8.6 Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
Privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.7 System Logs

Note: This request require Administrator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/syslog.cgi

Server will return the most up-to-date system log.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n

8.8 Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

http://<*servername*>/cgi-bin/admin/upgrade.cgi

Post data:

fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

8.9 Camera Control (capability.ptzenabled)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/camctrl.cgi?[channel=<value>][&camid=<value>]
[&move=<value>] – Move home, up, down, left, right
[&focus=<value>] – Focus operation
[&iris=<value>] – Iris operation
[&auto=<value>] – Auto pan, patrol
[&zoom=<value>] – Zoom in, out
[&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick
[&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick
[&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[[&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>][&speedlink=<value>]] – Set speeds
[&return=<return page>]

Example:

http://myserver/cgi-bin/camctrl/camctrl.cgi?channel=0&camid=1&move=right
http://myserver/cgi-bin/camctrl/camctrl.cgi?channel=0&camid=1&zoom=tele
http://myserver/cgi-bin/camctrl/camctrl.cgi?channel=0&camid=1&x=300&y=200&resolution=704x480&videosize=704x480&strech=1

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.

speedfocus	-5 ~ 5	Set the focus speed.
speedapp	-5 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
	stop	Stop zoom.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 8 <SD8362>	Set the speed of zooming, "0" means stop.
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.
vy	<integer>	
vs	0 ~ 127	Set the speed of movement, "0" means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.
videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system. 1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system.
focus	auto	Auto focus.
	far	Focus on further distance.
	near	Focus on closer distance.
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.10 ePTZ Camera Control (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value>
[&move=<value>] – Move home, up, down, left, right
[&auto=<value>] – Auto pan, patrol
[&zoom=<value>] – Zoom in, out
[&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick
[&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick
[&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[[&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>]] – Set speeds
[&return=<return page>]

Example:

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=0&move=right
http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&vx=2&vy=2&vz=2
http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&x=100&y=100&
videosize=640x480&resolution=640x480&stretch=0

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.
move	home	Move to home ROI.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop auto pan/patrol.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.

zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, "0" means stop.
vx	<integer>	The direction of movement, used for joystick control.
vy	<integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
x	<integer>	x-coordinate clicked by user. It will be the x-coordinate of center after movement.
y	<integer>	y-coordinate clicked by user. It will be the y-coordinate of center after movement.
videosize	<window size>	The size of plug-in (ActiveX) window in web page
resolution	<window size>	The resolution of streaming.
stretch	<boolean>	0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system. 1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedapp	1 ~ 5	Set the auto pan/patrol speed.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

8.11 Recall (capability.ptzenabled)

Note: This request requires Viewer privileges.

Method: GET

Syntax:

http://<*servername*>/cgi-bin/viewer/recall.cgi? recall=<value>[&channel=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
channel	<0~(n-1)>	Channel of the video source.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.12 ePTZ Recall (capability.eptz > 0)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>& recall=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
recall	Text string less than 40 characters	One of the present positions to recall.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

8.13 Preset Locations (capability.ptzenabled)

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/preset.cgi?[channel=<value>] [&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to the preset list.
channel	<0~(n-1)>	Channel of the video source.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.14 ePTZ Preset Locations (capability.eptz > 0)

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value> [&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
addpos	<Text string less than 40 characters>	Add one preset location to the preset list.

delpos	<Text string less than 40 characters>	Delete preset location from the preset list.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

8.15 IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax: <product dependent>

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?type[=<value>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<*ipaddress*>[&index=<value>][&return=<*return page*>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.
	delv6	Delete IPv6 address from access list.
ip	<IP address>	Single address: <IP address> Network address: <IP address / network mask> Range address:<start IP address - end IP address>
index	<value>	The start position to add or to delete.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

8.16 UART HTTP Tunnel Channel (capability.nuart > 0)

Note: This request requires Operator privileges.

Method: GET and POST

Syntax:

http://<*servername*>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]

GET /cgi-bin/operator/uartchannel.cgi?[channel=<value>]

x-sessioncookie: string[22]

accept: application/x-vvtk-tunnelled

pragma: no-cache

cache-control: no-cache

POST /cgi-bin/operator/uartchannel.cgi

x-sessioncookie: string[22]

content-type: application/x-vvtk-tunnelled

pragma : no-cache

cache-control : no-cache

content-length: 32767

expires: Sun, 9 Jam 1972 00:00:00 GMT

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through a proxy server.

This channel will help to transfer the raw data of UART over the network.

Please see UART tunnel spec for detail information

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.

8.17 Event/Control HTTP Tunnel Channel (capability.evctrlchannel > 0)

Note: This request requires Administrator privileges.

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrlevent.cgi
---------------------------------------------------------------------
GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache

---------------------------------------------------------------------
POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

8.18 Get SDP of Streams

Note: This request requires Viewer access privileges.

Method: GET/POST

Syntax:

http://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.

You can get the SDP by HTTP GET.

When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

8.19 Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<*servername*>/<network_http_s<0~m-1>_accessname>

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

8.20 Senddata (capability.nuart > 0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/senddata.cgi? [com=<value>][&data=<value>][&flush=<value>] [&wait=<value>] [&read=<value>]

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target COM/RS485 port number.
data	<hex decimal data>[,<hex decimal data>]	The <hex decimal data> is a series of digits from 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before read. no: Do not clear the receive data buffer.
wait	*1 ~ 65535*	Wait time in milliseconds before read data.
read	*1 ~ 128*	The data length in bytes to read. The read data will be in the return page.

Return:

HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n Content-Length: <system information length>\r\n \r\n <hex decimal data>\r\n

Where hexadecimal data is digits from 0 ~ 9, A ~ F.

8.21 Storage managements (capability.storage.dbenabled > 0)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>…]

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including *search*, *insert*, *delete*, *update*, and *queryStatus*.

Command: **search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes. Ex. mediaType='motion' Support trigger types are product dependent.
mediaType	<text>	Optional. Indicate the file media type. Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4'
resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'
isLocked	<boolean>	Optional.

		Indicate if the file is locked or not. 0: file is not locked. 1: file is locked. A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional. Indicate the event trigger time. (not the file created time) Format is "YYYY-MM-DD HH:MM:SS" Please embrace your input value with single quotes. Ex. triggerTime='2008-01-01 00:00:00' If you want to search for a time period, please apply "TO" operation. Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1st 2008 to the end of Jan 1st 2008.
limit	<positive integer>	Optional. Limit the maximum number of returned search records.
offset	<positive integer>	Optional. Specifies how many rows to skip at the beginning of the matched records. Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.

Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

Command: **delete**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1

Ex. Delete records whose key numbers are 1, 4, and 8.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8
```

Command: **update**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. retype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript

8.22 Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.

Method: GET

Syntax:

http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>]
[&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
vi<num>	state[(duration)nstate] Where "state" is 0, 1. "0"	Ex: vi0=1 Setting virtual input 0 to trigger state

	means inactive or normal state while "1" means active or triggered state. Where "nstate" is next state after duration.	Ex: vi0=0(200)1 Setting virtual input 0 to normal state, waiting 200 **milliseconds**, setting it to trigger state. Note that when the virtual input is waiting for next state, it cannot accept new requests.
return	<return page>	Redirect to the page <*return page*> after the request is completely assigned. The <*return page*> can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

Return Code	Description
200	The request is successfully executed.
400	The request cannot be assigned, ex. incorrect parameters. Examples: setvi.cgi?vi0=0(10000)1(15000)0(20000)1 No multiple duration. setvi.cgi?vi3=0 VI index is out of range. setvi.cgi?vi=1 No VI index is specified.
503	The resource is unavailable, ex. Virtual input is waiting for next state. Examples: setvi.cgi?vi0=0(15000)1 setvi.cgi?vi0=1 Request 2 will not be accepted during the execution time(15 seconds).

8.23 Open Timeshift Stream (capability.timeshift > 0, timeshift_enable=1, timeshift_c<n>_s<m>_allow=1)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]
```

For RTSP (MP4 and H264), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]
```

"n" is the channel index.

"m" is the timeshift stream index.

For details on timeshift stream, please refer to the "TimeshiftCaching" documents.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
maxsft	<positive interger>	0	Request cached stream at most how many seconds ago.
tsmode	normal, adaptive	normal	Streaming mode: normal => Full FPS all the time. adaptive => Default send only I-frame for MP4 and H.264, and send 1 FPS for MJPEG. If DI or motion window are triggered, the streaming is changed to send full FPS for 10 seconds. (*Note: this parameter also works on non-timeshift streams.)
reftime	mm:ss	The time camera receives the request.	Reference time for maxsft and minsft. (This provides more precise time control to eliminate the inaccuracy due to network latency.) Ex: Request the streaming from 12:20 rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30
forcechk	N/A	N/A	Check if the requested stream enables timeshift, feature and if minsft is achievable. If false, return "415 Unsupported Media Type".
minsft	<positive interger>	0	How many seconds of cached stream client can accept at least. (Used by forcechk)

Return Code	Description
400 Bad Request	Request is rejected because some parameter values are illegal.
415 Unsupported Media Type	Returned, if forcechk appears, when minsft is not achievable or the timeshift feature of the target stream is not enabled.

8. 24 Open Anystream (capability.nanystream > 0)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/videoany.mjpg?codectype=mjpeg[&resolution=<value>&mjpeg_quant=<value>&mjpeg_qvalue=<value>&mjpeg_maxframe=<value>]
```

For RTSP (MPEG4), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/liveany.sdp?codectype=mpeg4[&resolution=<value>&mpeg4_intraperiod=<value>&mpeg4_ratecontrolmode=<value>&mpeg4_quant=<value>&mpeg4_qvalue=<value>&mpeg4_bitrate=<value>&mpeg4_maxframe=<value>]
```

For RTSP (H264), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/liveany.sdp?codectype=h264[&resolution=<value>&h264_intraperiod=<value>& h264_ratecontrolmode=<value>& h264_quant=<value>& h264_qvalue=<value>& h264_bitrate=<value>& h264_maxframe=<value>]
```

<product dependent>

PARAMETER	VALUE	DEFAULT	DESCRIPTION
codectype	mjpeg, mpeg4, h264 <product dependent>	N/A	Set codec type for Anystream.
solution	capability_videoin_resolution	<product dependent>	Video resolution in pixels.
mjpeg_quant	0, 1~5 99, 1~5 <product dependent>	3	Quality of JPEG video. 0,99 is the customized manual input setting. 1 = worst quality, 5 = best quality. <product dependent>
mjpeg_qvalue	10~200 2~97 <product dependent>	50 <product dependent>	Manual video quality level input. (This must be present if mjpeg_quant is equal to 0, 99) <product dependent>
mjpeg_maxframe	1~25,	15	Set maximum frame rate in fps (for JPEG).

	26~30 (only for NTSC or 60Hz CMOS)		
mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	Intra frame period in milliseconds.
mpeg4_ratecontrolmode	cbr, vbr	vbr	cbr: constant bitrate vbr: fix quality
mpeg4_quant	0, 1~5 99, 1~5 <product dependent>	3	Quality of video when choosing vbr in "mpeg4_ratecontrolmode". 0,99 is the customized manual input setting. 1 = worst quality, 5 = best quality. <product dependent>
mpeg4_qvalue	1~31 2~31 <product dependent>	7 <product dependent>	Manual video quality level input. (This must be present if mpeg4_quant is equal to 0, 99) <product dependent> <product dependent>
mpeg4_bitrate	1000~8000000 1000~4000000 <product dependent>	512000 <product dependent>	Set bit rate in bps when choosing cbr in "mpeg4_ratecontrolmode".
mpeg4_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	10 15 <product dependent>	Set maximum frame rate in fps (for MPEG-4).
h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	1000	Intra frame period in milliseconds.
h264_ratecontrolmode	cbr, vbr	vbr	cbr: constant bitrate vbr: fix quality
h264_quant	0, 1~5 99, 1~5 <product dependent>	3	Quality of video when choosing vbr in "h264_ratecontrolmode". 0,99 is the customized manual input setting. 1 = worst quality, 5 = best quality. <product dependent>
h264_qvalue	0~51 <product dependent>	30 <product dependent>	Manual video quality level input. (This must be present if h264_quant is equal to 0, 99) <product dependent>
h264_bitrate	1000~8000000 1000~4000000	512000 <product	Set bit rate in bps when choosing cbr in "h264_ratecontrolmode".

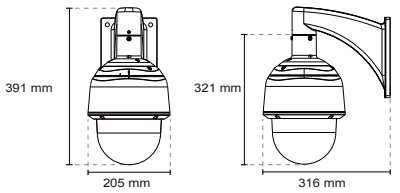
	<product dependent>	dependent>	
h264_maxframe	1~25, 26~30 (only for NTSC or 60Hz CMOS)	10 15 <product dependent>	Set maximum frame rate in fps (for H264).

Technical Specifications

Technical Specifications

Model	SD8333-E SD8333-EM (With Electric Dehumidifier)
System Information	
CPU	Multimedia SoC (System-on-Chip)
Flash	128 MB
RAM	256 MB
Camera Features	
Image Sensor	1/3" Progressive CMOS
Maximum Resolution	1280x720
Lens Type	30x Optical Zoom, Auto Focus
Focal Length	f = 4.3~129 mm (30x zoom)
Aperture	F1.6 ~ F4.7
Auto-iris	DC-iris
Field of View	2.1° ~ 57.8° (Horizontal) 1.2° ~ 34.5° (Vertical) 2.4° ~ 67.3° (Diagonal)
Shutter Time	1 sec. to 1/10,000 sec.
WDR Technology	WDR Pro
Day/Night	Removable IR-cut filter for day & night function
Minimum Illumination	0.15 Lux @ F1.6 (Color) 0.0048 Lux @ F1.6 (B/W)
Pan Speed	0.05° ~ 450° / sec
Pan Range	360 endless
Tilt Speed	0.05° ~ 450° / sec
Tilt Range	220° (-110° ~ +110°)
Preset Locations	256 preset locations, 40 presets per tour
Pan/tilt/zoom Functionalities	48x digital zoom (4x on IE plug-in, 12x built-in) Auto pan mode Auto patrol mode
On-board Storage	SD/SDHC/SDXC card slot
Video	
Compression	H.264, MJPEG & MPEG-4
Maximum Frame Rate	H.264: 60 fps @ 1280x720 MPEG-4: 60 fps @ 1280x720 MJPEG: 60 fps @ 1280x720 (Up to 30 fps in WDR mode)
Maximum Streams	4 simultaneous streams
S/N Ratio	Above 50 dB
Dynamic Range	110 dB
Video Streaming	Adjustable resolution, quality and bitrate Zoom enhancement for better image quality under limited bandwidth
Image Settings	Adjustable image size, quality and bit rate Time stamp, text overlay, flip & mirror Configurable brightness, contrast, saturation, sharpness, white balance, exposure control, gain, backlight compensation, privacy masks (Up to 24) Scheduled profile settings Defog
Audio	
Audio Capability	Audio input/output (full duplex)
Compression	AAC, G.711, G.726
Interface	External microphone input External line output
Network	
Users	Live viewing for up to 10 clients
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X
Interface	10Base-T/100BaseTX Ethernet (RJ-45) *It is highly recommended to use standard Cat. 5e & Cat. 6 cables which are compliant with the 3P/ETL standard.
ONVIF	Supported, specification available at www.onvif.org
Intelligent Video	
Video Motion Detection	Triple-window video motion detection
Auto-Tracking	Auto-tracking on moving object
Alarm and Event	
Alarm Triggers	Video motion detection, manual trigger, periodical trigger, system boot, recording notification, camera tampering detection, audio detection
Alarm Events	Event notification using digital output, HTTP, SMTP, FTP and NAS server File upload via HTTP, SMTP, FTP and NAS server
General	
Connectors	RJ-45 cable connector for Network/PoE connection Audio input Audio output AC 24V power input Digital input*4 Digital output*2 RS-485 for PTZ control (PelcoD protocol, Baud rate 2400)
LED Indicator	System power and status indicator
Power Input	PoE plus (IEEE 802.3at compliant) High Power PoE AC 24V
Power Consumption	PoE plus: Max. 19W AC 24V: Max. 48W (heater on) Max. 19W (heater off) High Power PoE: Max. 48W (heater on) Max. 19W (heater off)
Dimensions	Ø: 205 mm x 321 mm
Weight	Net: 3974 g
Casing	Weather-proof IP67- and NEMA 4X-rated mated housing Built-in electrical dehumidifier device (SD8333-EM)
Safety Certifications	CE, FCC Class A, VCCI, C-Tick, NEMA 4X
Operating Temperature	-5°C ~ 55°C (PoE Plus) -40°C ~ 55°C (AC 24V) -40°C ~ 55°C (High Power PoE)
Warranty	36 months
System Requirements	
Operating System	Microsoft Windows 7/Vista/XP/2000
Web Browser	Mozilla Firefox 7~10 (Streaming only) Internet Explorer 9.x or 10.x
Other Players	VLC: 1.1.11 or above Quicktime: 7 or above
Included Accessories	
CD	User's manual, quick installation guide, Installation Wizard 2, ST7501 32-channel recording software
Others	Wall mount bracket, screws, waterproof connectors, terminal blocks, quick installation guide, warranty card, alignment sticker, ground wire, T25 stardriver, software CD, desiccant bag

Dimensions



Compatible Accessories

Mounting Kits

AM-118
Indoor pendant head

AM-103
Recessed kit

AM-519
1.5" PT adapter

Power Adapter

AA-341
AC 24V Power Adapter

Others

AC-212/AC-111
Smoked cover/ Vandal proof transparent cover

AO-001
Combo cable

All specifications are subject to change without notice. Copyright © VIVOTEK INC. All rights reserved.

Distributed by:

Ver. 7

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho,
New Taipei City, 235, Taiwan, R.O.C.
T: +886-2-82455282 F: +886-2-82455532
E: sales@vivotek.com

VIVOTEK USA
2050 Ringwood Avenue,
San Jose, CA 95131
T: 408-773-8686 F: 408-773-8298
E: salesusa@vivotek.com

VIVOTEK Europe
Randstad 22-133, 1316BW Almere,
The Netherlands
T: +31(0)36-5298-434
E: saleseurope@vivotek.com

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準にづくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.